Re–Compression based JPEG Forgery Detection and Localization with Optimal Reconstruction

Diangarti Bhalang Tariang

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela–769 008, Odisha, India

May, 2016

Re–Compression based JPEG Forgery Detection and Localization with Optimal Reconstruction

A Thesis submitted in partial fulfillment

of the requirements of the degree of

Masters of Technology

in

Computer Science and Engineering

by

Diangarti Bhalang Tariang

(Roll Number: 214CS2144)

based on research carried out

under the supervision of

Dr. Ruchira Naskar

May, 2016

Department of Computer Science and Engineering

National Institute of Technology Rourkela
Rourkela–769 008, Odisha, India

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela–769 008, Odisha, India `www.nitrkl.ac.in`

May 17, 2016

Certificate of Examination

Roll Number: *214CS2144*
Name: *Diangarti Bhalang Tariang*
Title of Dissertation: *Re–Compression based JPEG Forgery Detection and Localization with Optimal Reconstruction*

We the below signed, after checking the dissertation mentioned above and the official record book of the student, hereby state our approval of the dissertation submitted in partial fulfillment of the requirements of the degree of ***Masters of Technology*** in ***Department of Computer Science and Engineering*** at ***National Institute of Technology Rourkela Rourkela–769 008, Odisha, India***. We are satisfied with the volume, quality, correctness, and originality of the work.

Ruchira Naskar
Supervisor

Santanu Kumar Rath
Head of Department

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela–769 008, Odisha, India www.nitrkl.ac.in

Dr. Ruchira Naskar
Assistant Professor

May 17, 2016

Supervisor's Certificate

This is to certify that the work presented in the dissertation entitled ***Re–Compression based JPEG Forgery Detection and Localization with Optimal Reconstruction*** submitted by ***Diangarti Bhalang Tariang***, Roll Number 214CS2144, is a record of original research carried out by her under my supervision and guidance in partial fulfillment of the requirements of the degree of ***Masters of Technology*** in ***Department of Computer Science and Engineering***. Neither this thesis nor any part of it has been submitted earlier for any degree or diploma to any Institute or University in India or abroad.

Ruchira Naskar

Dedicated to my family and my teachers for their endless love, support and encouragement. You mold me to a person I am becoming. All my achievements that I have or will accomplish in life is because you inspire me.

Declaration of Originality

I, ***Diangarti Bhalang Tariang***, Roll Number *214CS2144* hereby declare that this dissertation entitled ***Re–Compression based JPEG Forgery Detection and Localization with Optimal Reconstruction*** presents my original work carried out as a postgraduate student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

May 17, 2016
NIT Rourkela

Diangarti Bhalang Tariang

Acknowledgment

A two year journey to complete my thesis in obtaining my Master degree has come to an end. Along the journey I have come to learn new concepts and theories of my research work that only lead me to explore opportunities so as to challenge myself and be passionate about my work. At the end of my thesis journey, I belief I have successfully accomplished my tasks and desired results have been obtained. However I could not have succeeded without the support and encouragement of many. It would be an immense pleasure to express my gratitude to all who has contributed to the success of this thesis.

A profoundest gratitude to my supervisor, Dr. Ruchira Naskar. I have been indeed fortunate to work under her meticulous and scholarly guidance. She has been supportive since day one of my journey; regular meetings and deadline has been the impetus for the completion of my work. Her extensive guidance has given me the opportunity to gain insights into research activities. Her inspirational and motivational words inspired me in my scientific writing and publishing, for which I am grateful. My solemnest gratefulness to her.

My sincere gratitude to the H. O. D, Dr. Santanu Kumar Rath and all faculty members. Their academic support, timely cooperation and encouragement are greatly appreciated.

Many thanks to my friends for their generosity and support.

Most of all I thank my parents and my siblings for their unwavering support and encouragement to follow my dream. Their faith in me strengthens me and lifted me up whenever I was down. Their prayers for me has not been in vain. This accomplishment is theirs as much as is mine. There are no words to express of how much I thank them but I can only continue to pray that they be in good health.

Above all I thank my ***Heavenly Father*** for everything.

May 17, 2016 | *Diangarti Bhalang Tariang*
NIT Rourkela | Roll Number: 214CS2144

Abstract

In today's media–-saturated society, digital images act as the primary carrier for majority of information that flows around us. Such digital images have a profound impact on our lives as they play a significant role in providing evidences towards the faithfulness of any event. However image forgeries such as blurring, retouching, cropping, contrasting etc. have become extremely possible with the recent advent of highly sophisticated image processing tools that are easy–to–use and available at low–cost. The threat to the integrity and authenticity of digital images has been further increased by the fact that majority of the image manipulations done, are imperceptible, hence undetectable to human eyes. The authenticity and legitimacy of images are of prime importance and need to be protected. Hence the protection of image authenticity poses as a major challenge in today's digital world. Consequently, as a realization to the importance of identification of image forgery, in the recent years researchers have begun developing *Digital Image Forensic techniques*. In this thesis a blind digital forensic technique is proposed to detect manipulations as well as localize forgeries in digital images, blind in the sense that we require no original information of the image to detect the manipulations.

Today's most prevalent widely used image format as a world–wide standard for compression and storage is Joint Photographic Experts Group (JPEG). JPEG format, due to its efficient compression features and optimal space requirement, has acquired the use of almost all present-–day digital cameras. In this propose work we aim to detect malicious tampering of JPEG images, and subsequently reconstruct the forged image optimally. We deal with lossy JPEG image format in this paper, which is more widely adopted compared to its lossless counter–-part.

The first part of the thesis we devise a blind forgery detection and localization technique. The technique aims towards the detection and localization of not only a single forgery but also multiple forgeries within an image. The proposed work is based on finding an optimal error matrix image that clearly depicts the forged regions. Using varying values of compression factor the tampered image has been re–compressed and the difference between the its re–compressed versions and the original image are computed to obtain the error images. In the current literature survey, majority of the JPEG forgery detection techniques require the human interaction to select one out of many error images generated, that clearly depicts the existence of forgery. In this work we devise a technique that is capable of automatically finding that particular quality factor which generates the optimal error image.

Hence the entire JPEG forgery detection mechanism may be automated and successfully completed without human intervention, which is contrary to the operating principles of other JPEG forensic techniques.

In the next part of the thesis , we propose a technique to reconstruct the forged image optimally. We aim to achieve optimal reconstruction since the widely used JPEG being a lossy technique, under no condition would allow 100% reconstruction. The proposed reconstruction is optimal in the sense that we aim to obtain a close similarity form of the original image apart from eliminating the effects of forgery from the image.

For forgery detection and reconstruction of JPEG images, the inherent characteristics of JPEG compression and re–-compression features are exploited,

Proving the efficiency of our proposed technique we compare it with the other JPEG forensic techniques and using quality metric measures we assess the visual quality of the reconstructed image

Keywords: ***Digital forensics***; ***digital images***; ***Joint Photographic Experts Group(JPEG)***; ***re–compression***; ***image tampering***; ***tamper detection***; ***tamper localization***; ***JPEG reconstruction.***

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

In today's technology driven era, information and their exchange are extremely important for every aspect of our lives. High–speed transmission of information has been made possible by the widespread developments in information and communication technologies (ICTs). In today's media–saturated society, our day–to–day communication involves transmission and exchange of large volumes of digital images and videos as visual information over the internet as well as via broadcast and media, such news and television channels. Such visual information have a profound impact on our lives as they play a significant role in providing evidences towards the faithfulness of any event.

Photographs are historically known to act as eyewitnesses to affairs and events, and have gained people's trust over the ages. However, with the rapid rise in cyber–crime, information exchanged routinely over public channels have become highly vulnerable to interception and manipulation, which many times lead to wrong judgment. This is not tolerable in applications dealing with sensitive information, such as in legal and criminal investigations, political fields, medical, military and broadcast industries. The authenticity and legitimacy of images in such applications are of prime importance and need to be protected. Moreover image forgeries such as blurring, retouching, cropping, contrasting, etc. have become extremely possible with the recent advent of highly sophisticated image processing tools that are easy–to–use and available at low–cost. Such software and tools enable even a layman to retouch, edit or modify digital images according to his will, whether it is for legitimate use or a malicious act. For example Fig. 1.1 depicts a visually convincing forged image of a scene which questioned many at the time if US President Barack Obama was following the Indian politician Narendra Modi's campaign to be India's next prime minister [1]. With increased availability and sophistication of such tools, the trustworthiness of photography is diminishing day–by–day. The threat to the integrity and authenticity of digital images has been further increased by the fact that majority of the image manipulations done, are imperceptible, hence undetectable to human eyes. Hence the protection of image authenticity poses as a major challenge in today's digital world.

Consequently, as a realization to the importance of image authentication, as well as image

(a) Original image **(b) Forged image**

Figure 1.1: Altered Image Example(a) Authentic image (b) Forged image

source identification, in the recent years researchers have begun developing *Digital Image Forensic* techniques [2, 3]. *Digital Forensics* pertains to obtaining the legal evidences and footprints left behind in digital media, primarily for the purpose of cyber crime detection. Due to the growing importance of digital images in establishing trust towards any event, *Digital Image Forensics* has seen a rapid growth in the recent years [4–11]. The traditional techniques of protecting digital images against various security and privacy threats, such as *Digital Watermarking* [12–14] and *Steganography* [13–16], require special software or hardware chips to be embedded into the media capturing devices, which in turn alleviate the device cost manifolds. They require pre–processing of the data to be secured in some form or the other. However, digital forensic techniques do not have any apriori information requirement; all the investigations are done by post–processing of images. Hence such techniques constitute the class of *blind forgery detection* techniques [6, 17]. In this thesis work we are motivated to devise a new blind forgery detection scheme that can detect as well as localize forgeries within an image.

1.2 Problem Statement: JPEG Forgery

Digital cameras today, create and store images in specific formats. The most prevalent and widely used one, the Joint Photographic Expert Group (JPEG) due to its efficient compression features and optimal space requirement has acquired the use of almost all present–day digital cameras [18]. JPEG is a form of lossy image compression technique. However, due to the fact that changes in the components of an image pertaining to high frequency are less sensitive to the Human Visual System (HVS) [19] because of which, the JPEG compression process works by discarding most of the information contained in the high frequency components. This compression technique enables images to have considerably low storage requirement. However due to information loss, images saved in JPEG format undergo some amounts of degradations in their perceptual quality. The amount of degradation is determined by the level of compression, also known as the *compression ratio* or *JPEG quality factor* [18]. Higher the compression ratio, lower is the amount of image degradation.

JPEG being the most common image storage format used world–wide due to its best compression features and optimal space requirement, the recent years have seen a lot of research interest towards detection of JPEG forgeries [20–28]. JPEG forgery mainly happens in the following steps. (1) With the help of any image processing tool we open the JPEG image, (2) altering certain interesting parts of the image, and 3) saving the modified image as a JPEG file. Consequently, the re–-save operation leads to re–compression of the image. The effects of re–compression phenomenon involved in a JPEG image manipulation is one critical feature that majority of the JPEG forgery detection techniques exploit to detect the forgery. However not all JPEG re–compression processes signify tampering of an image. An image, simply opened and re–-saved as JPEG after legitimate modification, also undergoes re–-compression. In other words mere detection of the existence of re–compression is not sufficient to prove forgery. However, the acceptance of the modified image by the receiver, depends on whether the forged region(s) falls within or outside her Region of Interest (RoI). Therefore, localizing the tampered region(s) in an image is equally important and critical while detecting malicious tampering. JPEG forgery may be categorized into two classes, depending upon whether the Discrete Cosine Transform (DCT) structures of the preceding JPEG compression and that of succeeding JPEG compression are perfectly aligned or not with each other. We referred to them as *Aligned Double JPEG* (A–DJPG) compression based forgery in the first case and *Non–Aligned Double JPEG* (NA–DJPG) compression based forgery to that of the second case [29].

1.3 Objectives and Contributions

Our contributions in this thesis work are presented below:

- Our proposed work aims at detection and localization of both forms of JPEG tampering, *Aligned Double JPEG* (A–DJPG) compression based forgery and *Non–Aligned Double JPEG* (NA–DJPG) compression based forgery. The JPEG modification attack considered in this paper, may be modelled in the following way. An attacker selects some region of an image to manipulate. The attacker does the manipulations to the intended image region using some image editing software, after which she re–save the tampered image as JPEG file. In the process, due to the effects of re–compression the re–saved tampered region assumes a different compression ratio. This difference in compression ratios is exploited to detect and localize tampering in JPEG images. The technique aims towards the detection and localization of not only a single forgery but also multiple forgeries within an image.

- Majority of the JPEG forgery detection techniques present in the current state–of–the–art, require the human interaction to detect the existence of forgery. In this work we further devise a technique such that the entire JPEG forgery detection mechanism may be automated and successfully completed without human intervention.

- We also aim for subsequent reconstruction of the tampered JPEG image to a form closet to its original. The proposed reconstruction method aims at removing the forgery effects, the inconsistencies caused due to the presence of regions with varying compression ratios within a JPEG image. The proposed reconstruction method aims at transforming the tampered image to an image with uniform compression ratio throughout. Since the widely adopted JPEG compression technique is lossy in nature, 100% reconstruction of the image back to its originality is impossible. Therefore our reconstruction method works by transforming a tampered image optimally to an image with uniform compression ratio, i.e., to a form closet to its original. Hence we refer to it as optimal reconstruction of the tampered image. In other words, we aim to do an optimal reconstruction of tampered JPEG images.

1.4 Thesis Organization

This thesis is organized as follows. In Chapter 2 we present the reviews of the current state–of–the–art. In Chapter 3, we present a discussion on the JPEG compression technique, which is required for complete understanding of our work. In Chapter 4, we present a blind digital forensic technique for detection and localization of forgery in JPEG images. In Chapter 5, we propose an optimal reconstructing method for forged JPEG images. Experimental results are presented in Chapter 6, along with comparison with state–of–the–art and related discussion. Finally we conclude the paper with future research and directions, in Chapter 7.

Chapter 2

Literature Survey

Digital image forgery detection is broadly classified into two classes, namely, *active* or *non–blind* forgery detection [30–34] and *passive* or *blind* forgery detection [6, 17]. In active digital image forgery detection, watermarks or digital signatures are embedded at the time of capturing the images, which are later extracted and utilized for forgery detection and authentication. This is a constraint to their application to the digital image security, due to the fact that such techniques require specially equipped digital cameras with specific embedded software or hardware chips. Digital forensic approaches focus on passive forgery detection techniques, in order to secure and authenticate digital images without signatures or watermarks. Such techniques require no a–priori information processing or computation, hence termed as blind techniques. Such techniques are based on the fact that any attack delivered on an image, leaves behind some traces, which may be intelligently investigated and exploited in the future to detect image forgeries. For example, in [4], the author has shown how the underlying statistic properties of an image demonstrate various forms of inconsistencies, as a result of image forgery. Such inconsistencies are later on exploited by the author to detect the forgery.

Copy–move attack, is one of the primitive forms of image forgery. Singular Value Decomposition (SVD) and DCT was proposed by Zhao et al. [35] as a copy–move forgery detection method . To detect copied and moved blocks in an image lexicographic sorting technique have been used. *Image splicing*, where regions extracted from multiple images to form a single natural–looking composite, is another common form of image manipulation. Using edge sharpness as visual cues, Qu et al. [36] proposed system works by combining Order Statistic Filter (OSF) for measuring the edge sharpness, a feature extraction mechanism and a hierarchical classifier.

2.1 Double JPEG Forgery Detection

Any image undergoing forgery requires to be re–saved. The tampered image when re–saved as a JPEG file undergoes re–compression. However not all re-saving operations would indicate that an image has been tampered. An image, simply opened and re–saved as JPEG after legitimate modification, undergoes re–compression. Nevertheless, since most

JPEG forgeries involve at least a double JPEG compression, majority of JPEG forgery detection techniques in the current state–of–the–art are based on exploitation the effects of double JPEG compression [11, 20–28, 37–49].

JPEG forgery may be categorized into two classes, depending upon whether the Discrete Cosine Transform (DCT) structures of the preceding JPEG compression and that of the succeeding JPEG compression are perfectly aligned or not with each other. We referred to them as *Aligned Double JPEG* (A–DJPG) compression based forgery in the first case and *Non–Aligned Double JPEG* (NA-DJPG) compression based forgery to that of the second case [29].

2.1.1 A–DJPG Compression Forgery Detection Techniques

Significant techniques proposed for aligned JPEG forgery detection include [20, 21, 23–28, 37]. In [23, 24],using the generalized *Benford Distribution Law*, the statistical distribution of the first DCT quantized coefficients of every 8×8 DCT block of an image are analyzed for detecting JPEG re–compression. The first DCT quantized coefficient has specific changes when undergoing double re–compression with respect to the quality factor that is used for re–compression. The authors in [25, 26] detect JPEG re–compression by detecting periodic artifacts that are visible as double peak or periodic zero spectrum in the DCT coefficient histogram caused due to the difference in the configuration relationship between the first and second quantization step. The detection technique proposed by Lin et al. [27] and Bianchi et al. [28] provides improvements over the technique proposed by Popescu et al. [25] by locating tampered regions in the images based on the analysis of the DCT coefficients statistically. Also B. Mahdian and S. Saic in [37] proposed improvements to the work of Popescu et al. [25] by producing a significantly less number of false positives. Farid [20] proposed a technique of detecting double JPEG compression by having the tampered image be re–compressed using variable degrees of quality factors. The author investigated all the re–compressed images one–by–one, and found that the re–compressed version of the tampered image re–compressed wit the quality factor same as that used when re–saving the tampered image produced a *JPEG ghost* indicating the forged region. In [21] the authors have proposed technique that exploits consecutive pixel pair differences in JPEG ghost images for JPEG forgery detection.

2.1.2 NA–DJPG Compression Forgery Detection Techniques

Several researchers such as [22, 38, 42, 43, 46] have investigated and proposed techniques designed to detect non–aligned JPEG forgery. In [22] to detect the JPEG re–compressed block, the *Blocking Artifact Characteristics Matrix* (BACM) has been utilized. For authentic JPEG images the BACM exhibits symmetric blocking artifacts while they are asymmetric in the double compressed forged images. In [38] the authors have utilized the blocking artifacts in pixel domain; in their proposed work, the periodicity of blocking artifacts are analyzed using a binary blocking model. In [42, 43] the authors have exploited the integer periodicity maps and also computed the grid shift and quantization steps. The authors explored that the DCT coefficients tends to associate themselves around a predefined set of values. By measuring the degree of this association the authors are able to detect any shift in the DCT grids.

2.1.3 Combined Detection Technique of A–DJPG and NA–DJPG Compression Forgery

In [44], a technique capable of detecting image that had undergone tampering in either aligned form and mis–aligned form of JPEG forgery is proposed. This technique [44] operates by analyzing the periodical occurrences of blocking artifacts in non–aligned compression, whereas the periodical occurences of DCT coefficients artifacts in aligned compression. Another technique capable of detecting both aligned and non–aligned JPEG forgeries was proposed by [11]. In [11], based on a statistically improved and unified modelling of the artifacts that appear in an image undergoing both forms of aligned and non–aligned forgeries, the probability measurement of a DCT block that it undergone re–compression has been computed using the likelihood map technique.

2.1.4 JPEG Anti–forensics

Recently, a study of weaknesses and limitations of the current image forensics techniques shows that an intelligent forger with an advanced knowledge of forensic tools may conceal or remove traces of forgery. Such counter–attacks on forensic techniques, aimed to deceive forensic analyses, are combinedly referred to as *counter–forensics* or *anti–forensics* [50–54]. In [52, 53] Stamm et. al. proposed a JPEG anti–forensic method where redundancy values are added to the quantized DCT coefficients of the tampered image. By doing so, an image whose DCT distributions that matches the distribution of its original image is obtained thereby results in being not categorized as a forge image. However the distribution of redundancy values causes degradation in the image visual quality that can be detected by a total variation, TV–based detector [55] and the calibration–based detector [56]. Fan et. al. [54] proposed a variational based anti–forensic technique aiming to obtain an anti-forensic image with higher visual quality. The method defeats the TV–based and calibration–based detectors by employing a constrained total variation based minimization for de–blocking and feature value optimization.

Chapter 3

JPEG Compression Phenomenon

3.1 JPEG Compression and Decompression

In this section we provide a brief overview of JPEG compression and decompression techniques, for an 8-bit grayscale image. Our discussion is focused on those features of JPEG compression which are relevant to our work. For details of JPEG compression of images, the readers may refer to [18].

JPEG compression is constituted of the following steps:

1. An image is divided into 8×8 non–overlapping pixel blocks. Let us represent each such block by B (B = 1,2,3 ...,N).

2. Each block B then undergoes transformation on applying a two–dimensional Forward Discrete Cosine Transform (FDCT) to obtain its corresponding DCT coefficient block. Let $D^B(j,k)$, denote the DCT coefficient at entry (i,j) of block B, where $1 \leq j,k \geq 8$, .

$$D^B(j,k) = FDCT(B(j,k)) \tag{3.1}$$

3. The DCT coefficient $D^B(j,k)$ is uniformly quantized by:

$$QC_q^B(j,k) = round(\frac{D^B(j,k)}{Q(j,k)}) \tag{3.2}$$

   where the 8×8 matrix *Q* is the quantization matrix, and *Q(j,k)* is its $(j,k)^{th}$ entry termed as quantization step. The quantization matrix is defined by an integer quality factor q (q=1,2,$\cdots$,100).

4. The resultant quantized DCT coefficients QC are rearranged in zig-zag order and then encoded using a lossless encoding function such as Huffman Encoding [57].

5. JPEG decompression works by reversing the above compression method. The quantized DCT coefficients are decoded. Subsequently, the DCT coefficients are rearranged into 8×8 blocks, followed by dequantizing the coefficients. To recover the dequantized DCT coefficients we multiply the dequantized (i,j)th coefficients with the

corresponding quantization (i,j)th entries retrieving from the quality factor matrix.

$$QC_q^{-B}(j,k) = QC_q^{B}(j,k) \times Q(j,k) \tag{3.3}$$

6. The inverse DCT (IDCT) is applied on the dequantization coefficients QC^{-B}. The resultant values are rounded off to the nearest integers as:

$$B' = round(IDCT(QC_q^{-B}(j,k))) \tag{3.4}$$

7. Finally the grayscale values are truncated to the range [0,255], i.e., pixels assuming graylevel greater than 255 are made 255, and those assuming graylevel less than 0 are made 0, so that all pixels lie in the range [0,255] now. Note that, two forms of error which are involved in the JPEG decompression process, the rounding and truncation errors, make JPEG a lossy compression technique.

3.2 JPEG Re–Compression

As discussed previously in Chapter 1 and Chapter 2, when JPEG images are modified and re–saved they undergo at least two different JPEG compressions. When an image previously compressed at quality factor Q, undergoes re–compression with a quality factor Q', the resulting quantization coefficients become:

$$QC_{q'}^{B'}(j,k) = round(\frac{D^{B'}(j,k)}{Q'(j,k)}) \tag{3.5}$$

In the following subsections, we discuss the processes of *Aligned* and *Non–aligned* JPEG compression in more detail. During the proposed JPEG reconstruction, we require to distinguish aligned JPEG compression from its non–aligned counterpart.

3.2.1 Types of JPEG Re–Compression: Aligned and Non–Aligned

a Re–compressing a JPEG image such that the $* \times 8$ DCT grid of the two successive compressions are in phase with each other, then the image is said to exhibit *Aligned JPEG Compression* (A–JPG). A–JPG process is shown in Fig. 3.1(a). *Non–Aligned Double JPEG Compression* (NA–DJPG) occurs when some region(s) from an image is extracted and transplanted onto an image such that the DCT grid alignment is not in phase as shown in Fig. 3.1(b) (i). Subsequently, when the modified image is re–compressed, it undergoes non–aligned double JPEG compression. Another case of NA–DJPG, shown in Fig. 3.1(b) (ii), arises when the extracted region is re–compressed and later transplanted back to the original image.

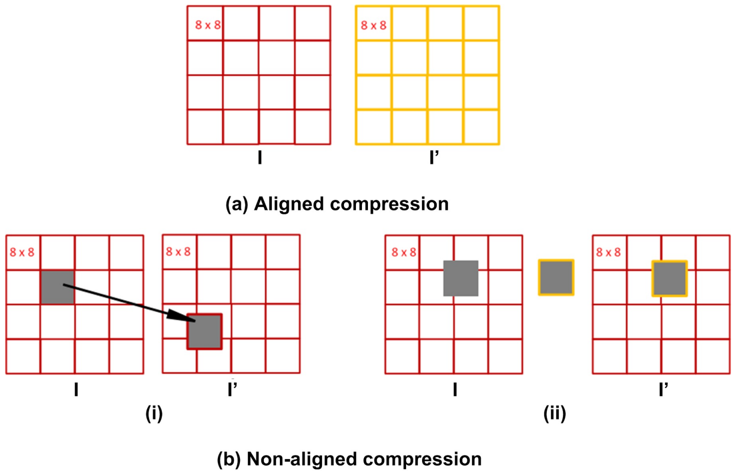


Figure 3.1: Aligned and non–aligned double JPEG compression. (a) Aligned compression where I is an image compressed with red DCT grids. Image I' is the recompressed version of I with yellow DCT grids aligned with the previous red DCT grids. (b) Non–Aligned Compression. (i) The highlighted block of image I is extracted and transplanted onto an image I' such that the DCT grid alignment is in phase (ii) The highlighted block of image I is extracted, re–compressed and transplanted back to image I, producing image I' without preserving grid alignment.

3.2.2 Same Quality Factor Re–Compression

Re–compressing a JPEG image using the same compression ratio (Q') as that used in the preceding compression (Q), i.e. when $Q' = Q$, changes in the pixel values are determined either by aligned compression or non–aligned compression. Next, we discuss the effects of re–compression with the same quality factor for the two types JPEG compression, one–by–one.

Aligned compression

The FDCT and IDCT functions are known to be the inverses of each other. In the case of aligned compression, the DCT coefficients $D^{B'}$ which is obtained by applying the FDCT function on the blocks of the image that is undergoing compression for the second time, (as obtained from Eq. 3.1) assume the same values as that of the dequantized coefficients QC_q^{-B} of the first compression process as obtained from Eq. 3.3 i.e:

$$D^{B'}(j,k) = QC_q^{-B}(j,k)$$

$$\implies D^{B'}(j,k) = QC_q^{B}(j,k) \times Q(j,k) \text{ [due to Eq. 3.3]} \tag{3.6}$$

Hence Eq. 3.5 of the double compression process with $Q' = Q$ becomes:

$$QC_q^{B'}(j,k) = round(\frac{QC_q^{B}(j,k) \times Q(j,k)}{Q(j,k)}) \tag{3.7}$$

During the JPEG dequantization process (Eq. 3.3, the dequantized coefficients are the exact multiplication values of the corresponding quantization entries. Since both DCT grids of the current and previous compressions are in phase, hence from Eq. 3.7, we have:

$$QC_q^{B'}(j,k) = QC_q^{B}(j,k) \tag{3.8}$$

Also when the second decompression process is applied, we have the dequantized DCT coefficients $QC_{q'}^{-B'}$ of the second compression equal to the dequantized DCT coefficients QC_q^{-B} of the first compression.

$$QC_q^{-B'}(j,k) = QC_q^{B}(j,k) \times Q(j,k) = QC_q^{-B}(j,k) \tag{3.9}$$

However due to the presence of quantization and rounding errors, there is a possibility that the corresponding image pixel values of the first compression and that of the second compression may differ in their grayscale values, their differences belonging to the range [-1,1]. Nevertheless the re–compressed image will be similar to its previously compressed version. In other words $S(j,k) = 0, \forall(j,k)$, where S represents the error matrix between the two compressed images, such that $S(j,k)$ stores the difference between the $(j,k) - th$ pixels of the two images.

Non–Aligned compression

In this form of double JPEG compression, some of the input blocks $B'(j,k)$ of the second compression process are not exactly the same as that of the output blocks $B'(j,k)$ of the first compression process. Due to which the FDCT function of the second compression process and the IDCT function of the first compression process are not the inverses of each other. Hence this form of compression forms the non–alignment in the corresponding DCT grids of the two successive compressions. The DCT coefficients of the second compression process (obtained from Eq. 3.1), differ considerably from the dequantized DCT coefficients obtained from Eq. 3.3 of the first compression i.e:

$$D^{B'}(j,k) \neq QC_q^{-B}(j,k) \tag{3.10}$$

Moreover, the DCT coefficients of the second compression are quantized with quantization step, indexed differently from the first compression. Therefore the corresponding pixel values of both the compressed images differ largely and the error matrix, S has its entries $S(j,k) \neq 0$ for most (j,k).

3.3 Summary

In this chapter the JPEG Compression features that are relevant to our work have been discussed. Aligned and non–aligned double compression features have been shown here.

When re–compression takes place using the exact values of the quantization matrix as that used in previous compression, change in pixels values depends on the compression type used. The characteristic of the error matrix S obtained by computing the differences between the corresponding pixels of the two compression images will be utilized in our proposed work.

Chapter 4

Tamper Detection and Localization in JPEG Images

While detecting JPEG image forgery, mere detection of the existence of double compression in the image is not convincing enough, since an image may have simply been opened and re–saved as JPEG after legitimate modifications to it, whereby it undergoes re–compression. Localizing the region(s)in an image that had undergone manipulations is significantly more critical and useful while detecting malicious tampering. In this case, the acceptance of the modified image by the receiver, depends on whether the tampered region(s) falls within or outside the *Region of Interest* (RoI) of the receiver. Summarily, we may assume that in general a tampered image has two regions, *unforged* and *forged*. During the recent years there have been significant researches related to localization of tampered region(s) in JPEG images [11, 21, 28, 47, 48]. In this section, we present in detail a blind JPEG forgery detection and localization technique, the preliminaries of which has been proposed by us very recently in [21]. In this paper, we additionally consider both cases of aligned and non–aligned JPEG forgeries, and extend the forgery detection and localization technique proposed in [21] to operate, specific to each case.

4.1 The JPEG Modification Model

The proposed JPEG forgery detection and localization technique assumes the following modification model. Let us consider the 512×512 *Lena* JPEG image shown in Fig. 4.1(a). Let QF_1 denoted the JPEG compression ratio of the original image.

1. We extract a region of the image, as depicted in Fig. 4.1(b) and re–save at a JPEG compression ratio QF_2 such that $QF_1 \neq QF_2$ and the image distortion is negligible perceptually.

2. Next, we transplant the extracted region back into the same location of the original image to produce the modified image, as depicted in Fig. 4.1(c). We save the tampered image in JPEG format with zero compression. In this paper, the research is solely towards the detection of JPEG image forgery that underwent re–compression of degree two, referred as *Double* compression. Re–saving the resultant image with compression

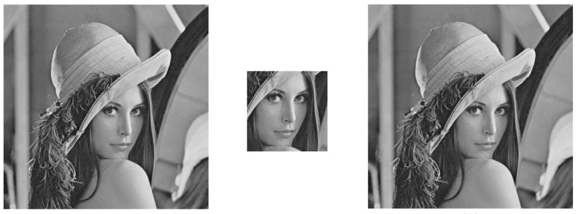


Figure 4.1: JPEG Attack on *Lena* image: (a)Authentic 512×512 image; (b) Region, re–saved at varying degrees of compression; (c) Tampered image with differently compressed regions.

ratio other than 100 would result in a different case of JPEG image forgery that is degree three compression or *Triple* compression [58]. Hence we save the resultant image with zero compression.

From Fig. 4.1(c) it is evident that the forged region having a compression ratio different from rest of the image, is perceptually indistinguishable. In the following sections, we present a blind technique to investigate the tampered image to distinguish the forged image regions from the unforged or authentic ones.

4.2 Detection of JPEG Forgery through Investigation of Image Differences

We now discuss our propose blind technique that detect the existence of forgery in JPEG images. First we investigate the differences between the forged image and different versions of it, obtained through re–compressions at varied JPEG quality factors. Let the tampered image be denoted by I. The following steps are carried out to compute the above–mentioned differences:

1. The tampered image is re–compressed at JPEG quality factor QF_x, where $QF_x = 40$. Let I_{QF_x} denote the image in its re–compressed version.
2. The error matrix S corresponding to I_{QF_x}, is computed as follows:

$$S(j,k) = [I(j,k) - I_{QF_x}(j,k)]^{10};\ j,k \leq 512 \tag{4.1}$$

3. The above steps 1 and 2 are repeated for QF_x ranging from 41 to 90 in steps of 1, and all the corresponding error matrices are stored for future investigation.

Next, we present the method of JPEG forgery detection through investigation of error matrices, and this detection is dependent on the type of forgery (aligned or non–aligned). According to the discussion in Section 3.2.2 of Chapter 3 when the tampered image is re–compressed with $QF_x = QF_1$ or $QF_x = QF_2$, the image pixel values undergo modifications, determined by the type of forgery, as we specify next.

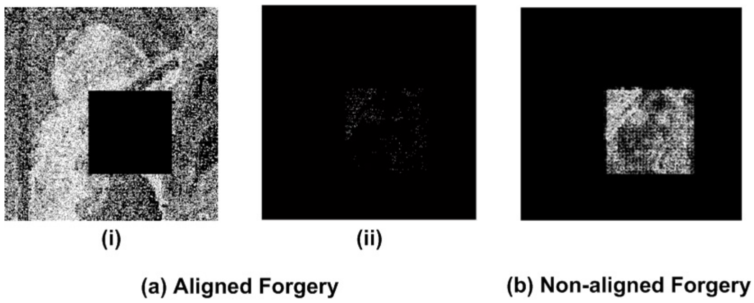


Figure 4.2: Error (S) images of *Lena*. (a) Aligned forgery case: (i) Error image at $QF_x = QF_2$. (ii) Error image at $QF_x = QF_1$. (b) Non-Aligned forgery case: Error image at $QF_x = QF_1$.

4.2.1 Investigation of Aligned Forgery

To investigate the existence of any aligned forgery in a JPEG image, the image is re–compressed with $QF_x = QF_2$ by the proposed method. Subsequently, the error matrix S is computed by Eq. 4.1. If the image is indeed tampered, the resultant error matrix S, when viewed as an image, allows the forged region to be distinguished clearly from the rest of the image in form of a dark patch, as visible in Fig. 4.2 (a) (i). This is due to the aligned compression characteristics discussed in Section 3.2.2 (a) of Chapter 3.

Also note here that, when the tampered image is re–compressed with $QF_x = QF_1$, the region of forgery is detectable and distinguishable as a dotted patch, brighter than the rest of the image, as shown in Fig. 4.2 (a) (ii).

4.2.2 Investigation of Non–aligned Forgery

When the tampered image is re–compressed with $QF_x = QF_1$ in non–aligned form, because the forged region has non–aligned compression characteristics, it is distinguishable in form of a brighter patch, from the rest of the image, which is now dark. This is evident from Fig. 4.2 (b).

4.3 Detection of JPEG Forgery through Automated Quality Factor Investigation

In the previous Section 4.2 we presented a JPEG forgery detection technique that is based on finding an optimal error matrix image that clearly depicts the forged regions. However the technique requires the human interaction to select one out of many error images generated, that clearly depicts the existence of forgery. In this section we devise a technique that is capable of automatically finding that particular quality factor which generates the optimal error image. Hence the entire JPEG forgery detection mechanism may be automated and successfully completed without human intervention, which is contrary to the operating principles of majority of the current state–of–the–art JPEG forgery detection approaches.

To do so, the differences of the forged image and different versions of it, obtained through re–compressions at varied JPEG quality factors, block–wise, where the size of each block is 8×8.

Let the tampered image of size N×N be denoted by I. Let us denote the actual compression ratio of an image as QF_1 and QF_x as the compression ratio used to re–compress the image. According to the discussion in Section 3.2.2 of Chapter 3 when the tampered image is re–compressed at QF_x, and the resultant error matrix S has $S(j,k) = 0\ \forall(j,k)$, we can infer that the preceding compression ratio QF_1 is equal to QF_x i.e. $QF_1 = QF_x$. If the tampered image is re–compressed with $QF_x = QF_1$, the error matrix S would have $S(j,k) = 0$ for authentic regions of the image, and $S(j,k) \neq 0$ for most forged regions. To detect the forgery we find the optimal error–matrix S for which most of its entries $S(j,k) = 0$. In other words, the forgery is detected by estimating the quality factors at varied regions of the image; and when most regions have quality factor equal to QF_1 the corresponding error—matrix is selected as the optimal one. This optimal error–matrix would clearly depict the existence of tampering in a tampered JPEG image. We formulate the following steps to detect the existence of tampering:

1. The tampered image is re–compressed at JPEG quality factor QF_x, where $QF_x = 40$. Let I_{QF_x} denote the version of the re–compressed image.

2. The error matrix S corresponding to I_{QF_x}, is computed as follows:

$$S(j,k) = [I(j,k) - IQF_x(j,k)]^{10} \text{ where } j,k \leq N. \tag{4.2}$$

3. Next, we divide the error matrix image, S into 8×8 non-overlapping pixel blocks $B_{(r,s)}$ row–wise, where $r, s = 1, 2, 3, \cdots, N/8$. The quality factor of each block denoted as $QF_{x,(r,s)}$ is estimated as:

$$\text{If } B_{(r,s)}(j,k) = 0,\ \forall(j,k),\ \ \leq j,k \leq 8, \text{ then}$$
$$QF_{x,(r,s)} \leftarrow QF_x.$$

4. The number of blocks having $QF_{x,(r,s)} = QF_x$, is recorded by a counter C_{QF_x}.

5. The above steps 1–4 are now repeated for QF_x = 41..90 in steps of 1. Hence, for all QF_x in 40..90, the corresponding number of image blocks having matching quality factors are recorded in $C_{40}..C_{90}$.

6. The desired optimal quality factor (QF_o) at which the optimal error–matrix image will be generated, would correspond to the maximum of $C_{40}..C_{90}$, i.e.,

$$QF_o \leftarrow QF_x$$

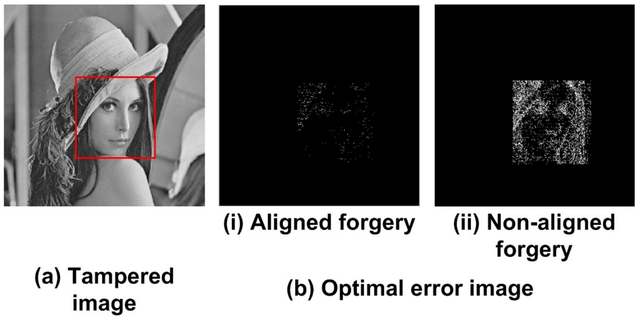


Figure 4.3: Forgery Detection for *Lena* JPEG image of size 512×512 pixels. (a) Tampered image: the central forged region of has been outlined; (b) Optimal error–matrix image depicting the existence of tampered most clearly at $QF_o = QF_1$ (i) Aligned forgery (ii) Non-aligned forgery.

such that $C_{QF_x} = maximum(C_{40}, C_{41}, \cdots, C_{90})$.

If the image is indeed tampered, the resultant error matrix S obtained using Eq. 4.2 by re–compressing the image at QF_o, when viewed as an image, allows the forged region to be distinguished clearly in form of a grayish dot like pattern.

Shown in Fig. 4.3 (a) is a *Lena* JPEG image of size 512×512 pixels with original JPEG quality be QF_1 (say), from which a region was extracted, re–compressed at a compression factor (say) QF_2 and transplanted back to the same location of the original. Fig. 4.3 (b) shows the optimal error–matrix corresponding to the automatically generated optimum quality factor, which happens to be $QF_o = QF_1$. The image in Fig. 4.3 (b)(i) for the case of aligned forgery and Fig. 4.3 (b)(ii) for the case of non-aligned forgery show the modified image region very clearly.

4.4 Localizing the Tampered Regions

In this section, we describe the method of identifying and localizing the region(s) having different compression ratio(s), compared to the rest of the image. As discussed in Section 4.2 and Section 4.3, the presence of tampering in both cases of aligned and non–aligned forgeries can be detected from the error image generated when the tampered image is re-compressed with $QF_x = QF_1$.

The following procedure utilizes this information to identify the forged regions:

1. First we re–compresse the forged image at JPEG compression factor QF_x, where $QF_x = QF_1$. Let I_{QF_1} denote the version of the re–compressed image.

2. The error matrix S corresponding to I_{QF_1}, is computed using Eq. 4.1 as follows:

$$S(j,k) = [I(j,k) - I_{QF_1}(j,k)]^{10} \text{ where } j,k \leq 512.$$

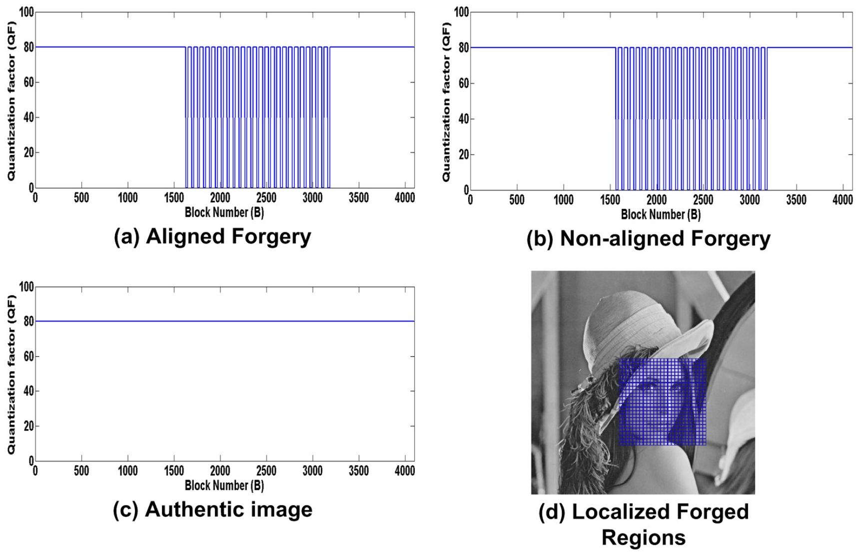


Figure 4.4: Localization of forged regions where the tampered region was compressed at an unknown quality factor, different from the original quality factor (QF_1) (a) QF vs. B plot for aligned forgery; (b) QF vs. B plot for non-aligned forgery; (c) QF vs. B plot for authentic image; (d) Marked region indicating the localized tampering.

3. Next we divide the error matrix image, S is divided into 8×8 non-overlapping pixel blocks $B_{(r,s)}$, where $r, s = 1, 2, 3, \cdots, 64$. According to the discussion in Section 3.2.2, when an image is r–compressed at QF_x and the resultant error matrix S has $S(j,k) = 0 \;\forall (j,k)$, we can infer that the preceding compression ratio QF_1 is equal to QF_x, i.e., $QF_1 = QF_x$. For a tampered image, the error matrix S would have $S(j,k) = 0$ for authentic regions of the image, and $S(j,k) \neq 0$ for forged regions. Utilizing this error information, each block of the tampered image is investigated to find if it assumes a quality factor equal to QF_1, as follows:

$$If\ B_{(r,s)}(j,k) = 0,\ \forall (j,k),\ 1 \leq j,k \leq 8\ ,$$

$$Then\ QF_{(r,s)} \ \leftarrow\ QF_1 \tag{4.3}$$

$$Else\ QF_{(r,s)} \ \leftarrow\ 0 \tag{4.4}$$

Next we plot the quality factor ($QF_{(r,s)}$) against the block number ($B_{(r,s)}$). This plot helps us to locate the exact blocks which are forged in a JPEG image. The QF vs. B plot for the manually forged Lena image as shown in Fig. 4.1 (c), has been presented in Fig. 4.4. The QF vs. B plot provides an evidence to the existence of forgery, if any, as well as indicates the location of forgery, which can be investigated in the following way. In both cases of aligned and non–-aligned forgery detection, the plots demonstrate sudden changes in the QF vs. B characteristics, where a range of blocks exhibit unknown quality factor values different from

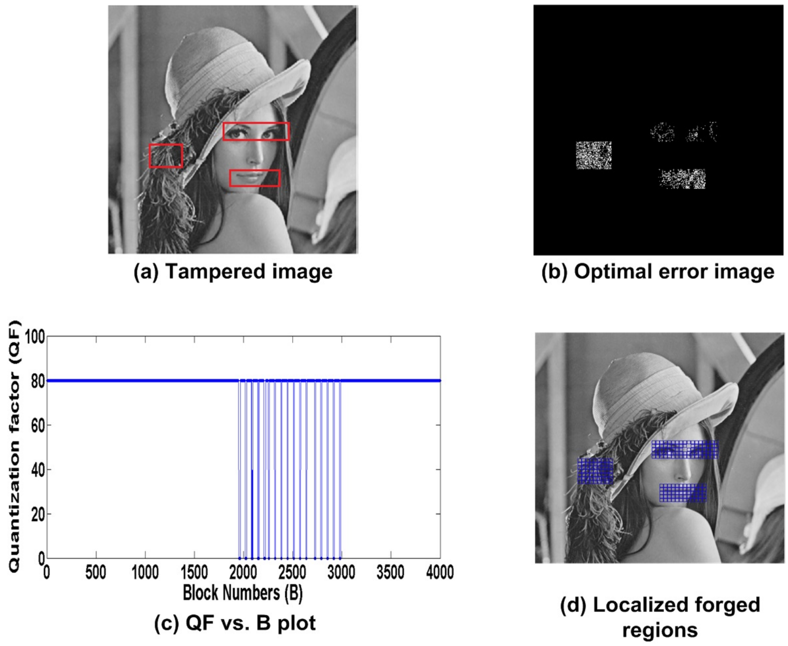


Figure 4.5: Multiple forgeries detection and localization in 512×512 *Lena* JPEG image. (a) The tampered image: (manually) forged regions outlined; (b) Optimal error image depicting the existence of forgery; (c) QF vs. B plot; (d) Localized tampered regions

the rest of the image blocks (whose quality factor has been estimated to be equal to QF_1). The sudden change remain persistent over a range B, and this range corresponds to the region that has undergone forgery. In the QF vs. B plot we have indicated the unknown quality factor to be zero. This has been shown in Fig. 4.4 (a) and Fig. 4.4 (b). Furthermore, we localized the forged region by recording the block indices (B) with unknown quality factor i.e $QF = 0$. The localized tampered regions (corresponding to Fig. 4.1 (c)) are shown in Fig. 4.4 (d). The QF vs. B characteristics for the authentic Lena image demonstrates a single line plot at $QF = QF_1$, indicating that the entire image is evenly compressed with the same quality factor.

4.5 Handling Multiple Forgeries

A practical assumption in regard to JPEG forgery detection, is considering the possibility of a single JPEG consisting of multiple forgeries, where multiple regions of the image are manipulated. Next we further discuss the flexibility and capability of the proposed detection and localization techniques to handle multiple forgeries in a single JPEG.

We have considered a generalized JPEG *multiple* forgery model, in the sense that the multiple forgeries involve re–compressions at varying quality factors within the image. The proposed detection and localization methods presented in the previous sections when applied on the tampered image with multiple forged regions, enable us to detect all those regions individually. These are visible in the error image S, as well as the QF vs. B plots. The QF vs. B plots enable us to localize the exact regions of all forgeries in an image. Shown in Fig. 4.5 (b) is an optimal error image obtained at $QF_x = QF_1 (QF_1$ is the original quality factor of the image) that depicts the existence of forgeries. Fig. 4.5 (c) depicts the QF vs. B plot. Shown in Fig. 4.5 (d) is the localized result of the forged regions.

4.6 Summary

In this chapter we proposed a JPEG forgery detection and localization techniques. The inherent characteristics of JPEG compression and the effects of re–-compression have been exploited in order to detect and localize forgery. The series of S error images have been investigated to find the optimal error–image for which most of its entries $S(j,k) = 0$. The optimal error–matrix clearly depicts the existence of forgery in a tampered image. We utilize the optimal error image. The tampered image has been divided into blocks of 8×8 pixels and the quality factor (QF) of each block is estimated. The QF vs. B plot is used to localize the forgeries by locating those blocks with unknown quality factor.

Chapter 5
Reconstruction of Forged Image

In this section we devise a method for optimal reconstruction of tampered JPEG images. The results of tamper detection and localization, as obtained in Chapter 4 have been utilized here. Our proposed reconstruction method aims at removing the forgery effects, the inconsistencies caused due to the presence of multiple compression ratios within a single JPEG image. Our reconstruction method aims of transforming the tampered image to an image with uniform compression ratio. Since the widely adopted JPEG compression technique is lossy in nature, 100% reconstruction of the image back to its originality is impossible. Therefore our reconstruction method works by transforming a tampered image to one with uniform compression ratio. The transformed JPEG image is supposed to be an optimal reconstruction of the forged JPEG, which is closest to its original authentic form.

To reconstruct the forged image, we first identify the forged and unforged regions of it, by the results obtained from Chapter 4. Now, the forged and the unforged regions are further investigated so as to find out their respective compression ratios. Let us assume that the forged image I has two regions with different compression ratios (according to our attack model in Section 4.1 of Chapter 4). Let us denote the unforged region as I_1 singly compressed with quality factor QF_1, and the forged region of size m×n pixels with I_2 doubly compressed consecutively at quality factors QF_1, QF_2. Because the widely used JPEG format is lossy, reconstructing the image back to its original compressed ratio i.e QF_1 has not been considered in this work. Instead, the double compression ratio (QF_1, QF_2), at which I_2 had been compressed, is considered for reconstructing the image. Fig. 5.1 depicts the proposed model of reconstructing the forged image. The image in Fig. 5.1 (a) is the authentic image with quality factor QF_1. In Fig. 5.1 (b) as depicted is a forged image with a region of it re–compressed with quality factor QF_2, thereby consecutively compressed at QF_1, QF_2. Finally, as illustrated in Fig. 5.1 (c) the forged image is reconstructed such that the entire image now assumes a uniform compression ratio same as QF_1, QF_2 combined. This has been

The following sections provides the discussion of the procedure of reconstructing the image, as discussed above.

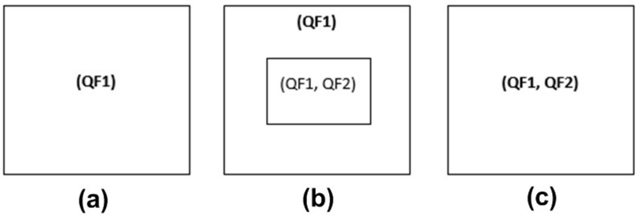


Figure 5.1: Modeling the proposed reconstruction. (a) Original image compressed at quality factor QF_1.(b) Forged image with forged region re–compressed at QF_2. (c) Entire image reconstructed, now assuming uniform compression ratio (QF_1, QF_2).

5.1 Determination of Quality Factor

When investigating the tampered image, the ratios at which the regions were compressed are unknown and to reconstruct the image we require the knowledge of their values. From the results obtained in Section 4.2 and Section 4.4 of Chapter 4, the forged and unforged regions are successfully identified. Also in Section 4.4 the compression ratio at which the unforged region I_1 is compressed has been estimated and found to be equal to QF_1, the actual compression compression ratio of the original JPEG image. Next we describe the procedure to expose out the compression ratio of the forged region I_2 of a tampered image I.

According to the discussion in Section 3.2.2 of Chapter 3 re–compressing a JPEG image at QF_x, and the resultant error matrix S has $S(j,k) = 0 \; \forall (j,k)$, we can infer that the preceding compression ratio QF_1 is equal to QF_x i.e. $QF_1 = QF_x$. In this section we utilize this error matrix information to determine the compression ratio of the forged regions through the following steps. (As before, we denote the compression ratio of the unforged region by QF_1 and that of the forged region by QF_1, QF_2.)

1. We re–compress the entire image I at varying compression ratios (QF_x) in the range [40,90], to obtain different re–compressed images I_{QF_x}.

2. For each value of QF_x, do steps 3–5.

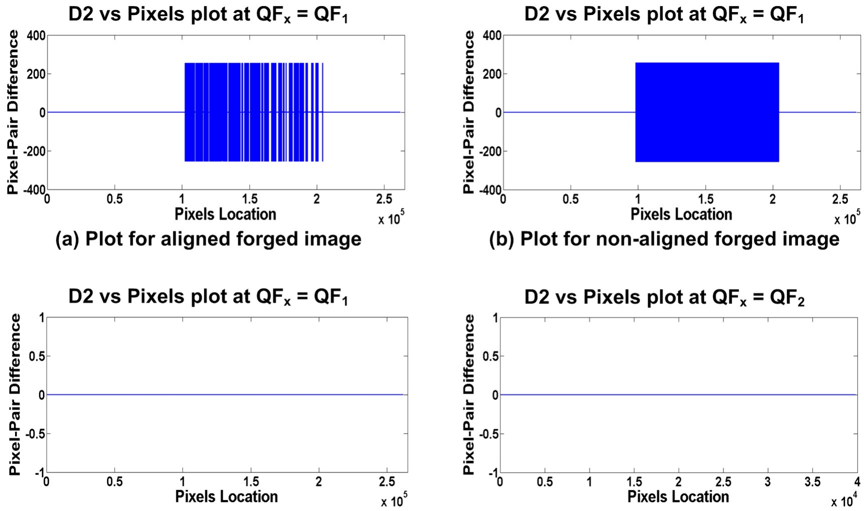
3. We compute the error matrix S between an image I and its re–compressed version I_{QF_x} using Eq. 4.1 i.e.

$$S(j,k) = [I(j,k) - I_{QF_x}(j,k)]^{10}; \; j,k \leq 512$$

4. Next, the consecutive horizontal pixel–pair differences (D_2) of the error image S, is computed row–wise, as follows:

$$D_2 = \{S(j,k) - S(j,k+1) : 1 \leq j \leq 512; \; 1 \leq k \leq 511\} \tag{5.1}$$

where S denotes the error matrix (computed by Eq. 4.1) and $S(j,k)$ denotes the $(j,k)^{th}$ pixel of S. D_2 is a vector used to store the pixel–pair differences of S. Note here, that



(a) Plot for aligned forged image

(b) Plot for non-aligned forged image

(c) Plot for authentic image

(d) Plot for forged region

Figure 5.2: The $D_2\ vs.\ Px$ plot for Lena image. (a) Plot for aligned forgery for $QF_x = QF_1$; (b) Plot for non–-aligned forgery for $QF_x = QF_1$; (c) Plot for authentic Lena image for $QF_x = QF_1$; (d) Plot corresponding to the forged (extracted) region for $QF_x = QF_2$.

the pixel–pairs are considered row–wise, horizontally. Therefore D_2 has 512×511 elements: $[D_2(1), D_2(2), \cdots, D_2(512 \times 511)]$.

5. Let xP be another horizontal vector denoting the pixel indices in a 512×511 matrix. Hence xP = [1, 2, 3, . . ., 512×511]. Next, we plot the vector of pixel–pair differences, D_2 against xP.

6. For $QF_x = 40..90$, we investigate all D_2 vs. xP plots, .

The D_2 vs. xP characteristics for the authentic *Lena* image (originally compressed at compression ratio QF_1, has been shown in Fig. 5.2 (c). Also the D_2 vs. xP plot for the forged *Lena* image of Fig. 4.1 (a), has been presented in Fig. 5.2 (a) in case of aligned forgery and Fig. 5.2 (b) in case of non–aligned forgery. In both cases of aligned and non–aligned forgery detection, the plots (for $QF_x = QF_1$) demonstrate sudden changes in the D_2 vs. xP characteristics, which remain persistent over a range of xP, and this range corresponds to the region that has undergone forgery.

On analyzing the D_2 vs. xP plots for the authentic *Lena* image, as shown in Fig. 5.2 (c), we see that it demonstrates a zero line plot. This zero plot was obtained for $QF_x = QF_1$, where QF_1 is the compression ratio of the original image and QF_x is its re–compression ratio. The zero line D_2 vs. xP plot provides an evidence to the fact that the image has a uniform compression ratio, equal to QF_1. Based on this finding, we aim to find out the compression ratios of those region(s) whose compression ratios differ from rest of the image. The underlying compression ratio is given by that specific value of $QF_x \in [40, 90]$, which produces a zero line D_2 vs. xP plot, as shown in Fig. 5.2 (d).

In order to find out the quality factor at which the forged region was compressed, we utilize the localization results obtained in Section 4.4 to extract the forged region I_2 separately from the tampered image I. Next we apply the above steps 1–7 on the extracted region.

In case of non–aligned forgery, the above steps 1–7 are performed similarly. However, the D_2 vs. xP plot may not demonstrate a zero line. This is due to the fact that the forged region is mis–aligned from the 8×8 image DCT grids by r rows and c columns, where $0 \leq r \leq 7$ and $0 \leq c \leq 7$ but $r \neq 0, c \neq 0$. Hence, to determine the quality factor in this case, the localized forged region is shifted by $0 \leq r \leq 7$ rows and $0 \leq c \leq 7$ columns except $r = 0, c = 0$, from left to right and top to bottom; that is all 63 possible shifted versions are now considered. We are bound to obtain a zero line D_2 vs. xP plot for at least one of the shifted versions, for one specific value of QF_x, as shown in Fig. 5.2 (d). This value of QF_x, represents nothing but the forged region's re–compression ratio.

5.2 Single Compression Ratio Reconstruction of Forged JPEG Images

Next we devise the steps to reconstruct the entire image optimally. Our aim here is to "level out" the regions of a tampered JPEG image, hence transform it to another JPEG image which has a uniform compression ratio QF_1, QF_2 throughout.

Based on the type of forgery, aligned or non–aligned, reconstruction of the forged image is discussed next.

5.2.1 Reconstruction for Aligned Forgery

A JPEG image which has undergone aligned forgery, is reconstructed by the proposed method, through the following steps. In the following, I denotes the forged image, and as before, we denote the compression ratio of the unforged region of I by QF_1 and that of the forged region by QF_1, QF_2.

1 First, the entire image I is re–compressed at the compression ratio QF_2 to generate image I_r. (Note that the forged region has now been consecutively compressed at (QF_1, QF_2, QF_2) and the unforged region at (QF_1, QF_2), in image I_r.)

2 Second, the forged region of image I_r is replaced by the corresponding pixels value of the forged region of image I i.e.,

$$I_r(i,j) \leftarrow I(i,j), \forall I(i,j) \text{ belonging to the forged region of the image} \tag{5.2}$$

Note that, now we have the entire image reconstructed at an uniform compression ratio (QF_1, QF_2), combined.

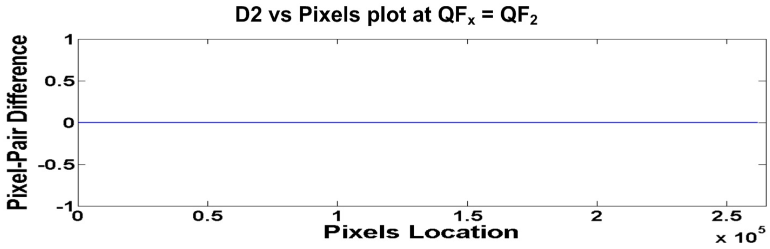


Figure 5.3: D_2 vs. xP plot for the reconstructed *Lena* image in case of aligned forgery.

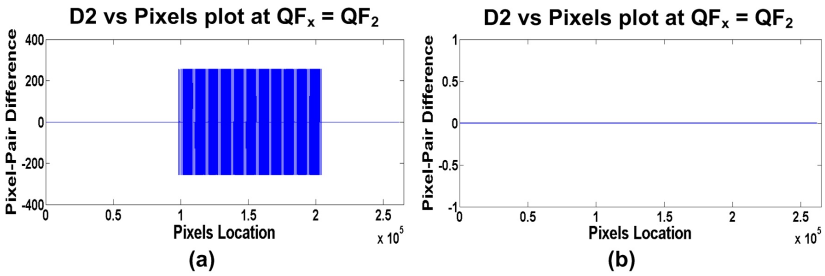


Figure 5.4: D_2 vs. xP plot for the reconstructed *Lena* image in case of non–aligned forgery. (a) Expected abrupt change in the D_2 vs. xP plot. (b) D_2 vs. xP plot of the final reconstructed image.

Finally, the D_2 vs. xP plot for the reconstructed image I_r is generated with re–compression ratio $QF_x = QF_2$. This plot demonstrates no sudden change, rather depicts a zero line characteristic, which is same as that of the authentic image. The D_2 vs. xP plot for I_r with $QF_x = QF_2$ has been shown in Fig. 5.3

5.2.2 Reconstruction for Non–aligned Forgery

For reconstruction in case of non–aligned forgery, we perform the same steps 1–2 as in the case of aligned forgery reconstruction, discussed in Section 5.2.1. However, in the case of non–aligned forgery, the D_2 vs. xP plot still demonstrates non–zero D_2 values corresponding to the forged region. This has been shown in Fig. 5.4(a). As evident from Fig. 5.4 (a), there is a sudden change in D_2 values, persistent over a range of xP values, corresponsing to the forged region.

This suggests that in spite of replacing the forged region of the reconstructed image I_r, with the forged region of tampered image I, a zero line D_2 vs. xP characteristic could not be achieved for I_r. This is due to the the mis–alignment of DCT grids at the time, the tampered region was extracted and replaced (in step 2), from that when the entire image was re–compressed at QF_2 (in step 1) according to the definition of non–aligned forgery. (This phenomenon has been discussed in more detail with justification in Section 3.2.2). Hence, in order to reconstruct the image in case of non–aligned forgery, after steps 1–2 presented in Section 5.2.1, we perform the following steps 3–6:

3 The rise in D_2 vs xP plot shown in Fig. 5.4(a) is forcefully leveled down to zero, i.e., we assign $D_2(i) \leftarrow 0 \,\forall 1 \leq i \leq 512 \times 511$.

4 From the resultant plot (specifically the D_2 values) obtained after performing step 1 above, we *backtrack* and compute the error matrix S' as:

$$S'(j,k) = [S(j,k-1) - S(j,k-1)] \,\forall\, 1 \leq j \leq 512,\ 2 \leq k \leq 512,\ S'(1,1) = S(1,1) \tag{5.3}$$

5 From the error matrix S' we *backtrack* and reconstruct the pixel values of the image I_r' as follows:

$$I_r'(j,k) = round(\sqrt{S'(j,k)}) - I_r(j,k), \quad j,k \leq 512 \tag{5.4}$$

6 Finally, the pixel–pair differences (D_2) of I_r' are computed and plot against the pixels indices (P) for $QF_x = QF_2$. As evident from Fig. 5.4 (b), this plot now demonstrates a zero line, hence indicating that the reconstruction is complete.

5.3 Summary

In this chapter we propose a method to reconstruct a tampered JPEG image (having varying quality factors), hence transform it into a form having uniform quality factor throughout. However, due to inherent lossy property of JPEG compression, it is not possible to remove the effects of double–compression from the tampered image, however we succeed to remove the differences in quality factors. Hence we call it an *optimal* reconstruction of JPEG images. To reconstruct the forged image we utilize the characteristics of the pixel–differences D_2 computed from the S error matrix. The $D2$ vs. xP plot of a reconstructed JPEG image demonstrates a zero line consistent to that of an original image. Thus the resultant reconstructed image with uniform quality factor has been optimally reconstructed.

Chapter 6

Experimental Results And Discussion

The proposed technique is implemented in MATLAB, using the MATLAB *Image Processing Toolbox*. For our experiments, shown in Fig. 6.1 are the 16 standard 512×512 grayscale images collected from CVG-UGR Image Database [59] and USC-SIPI Image Database [60]. To perform compression of the test JPEG images with specific compression ratios we have used the `imwrite` function of MATLAB. The `imwrite` function of MATLAB allows JPEG quality factors in the range [1,100], '100' representing zero compression and '1' representing the maximum level of compression.

In our experiments we have used JPEG images compressed at quality factor $QF_1 \in [40, 90]$. We have manually forged selected regions of the test images for our experiments, the manual forgery being induced in the following way. We extracted a $m \times n$ region of the image, where $1 \leq m, n < 512$ and re–saved it with a second quality factor $QF_2 \in [40, 90]$. The re–compressed region is later transplanted back to the same locationof the original image.

To illustrate the effectiveness of the proposed method over JPEG forgeries involving diverse compression ratios, the attack on the above–mentioned test images have been conducted manually by considering diverse values of QF_1 and QF_2. The experimental results to follow, prove the efficiency of the proposed methods in all above cases.

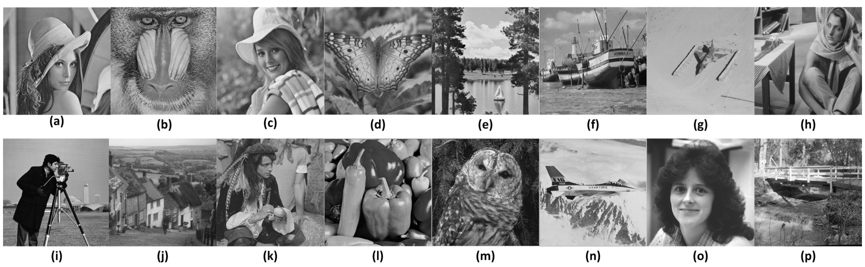


Figure 6.1: Grayscale test images(512×512 pixels) (a) *Lena* (b) *Mandrill* (c) *Elaine* (d) *Butterfly* (e) *Lake* (f) *Boat* (g) *Jetplane* (h) *Barbara* (i) *Cameraman* (j) *Goldhill* (k) *Pirate* (l) *Peppers* (m) *Owl* (n) *Airplane* (o) *Woman darkhair* and (p) *Walkbridge*.

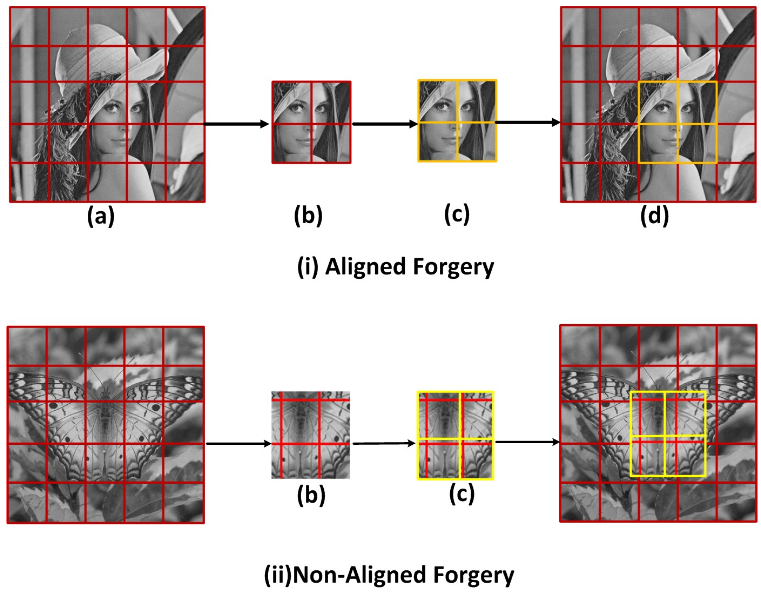


Figure 6.2: (i) Aligned Forgery. (a) Lena image originally compressed; DCT grids shown in red. (b) Extracted region preserving DCT grids. (c) Extracted region re–compressed; DCT grids shown in yellow. (d) Forged image with *aligned* DCT grids. (ii) Non–aligned Forgery. (a) Butterfly image originally compressed; DCT grids shown in red. (b) Extracted region, *not* preserving DCT grids. (c) Extracted region re–compressed; DCT grids shown in yellow. (d) Forged image with *mis–aligned* DCT grids.

6.1 Forgery Detection and Localization Results

In our experiments we have considered both cases of aligned and non–aligned JPEG attack. Specifically,

1. For aligned forgery, the selected region is extracted such that all its boundary pixel location coincides with the DCT grid of the original image. In our experiment, we select and extract a 200×200 region of a 512×512 test image, located at pixel position (201:400,201:400) (i.e from row 201 to 400 and column 201 to 400) to be tampered (intentionally) . The aligned forgery attack on *Lena* image is shown in Fig. 6.2 (i).

2. For non–aligned forgery, the image region to be tampered is selected such that it does not preserve the DCT grid alignment of the original image. In our experiment, the region located at pixel position (200:399,200:399) is selected for manual tampering. This has been shown in Fig. 6.2 (ii), for the *Butterfly* image.

Now, the tampered images are analyzed for forgery detection and localization. As discussed in Section 4.2, the forged images undergo re–compressions at different values of quality factor QF_x, ranging from 40 to 90 in steps of 1. The corresponding error images (S matrices) are computed using Eq. 4.1. The error images for varying degrees of re–compression in the range [40,90], for the *Lena* test image have been depicted in Fig. 6.3

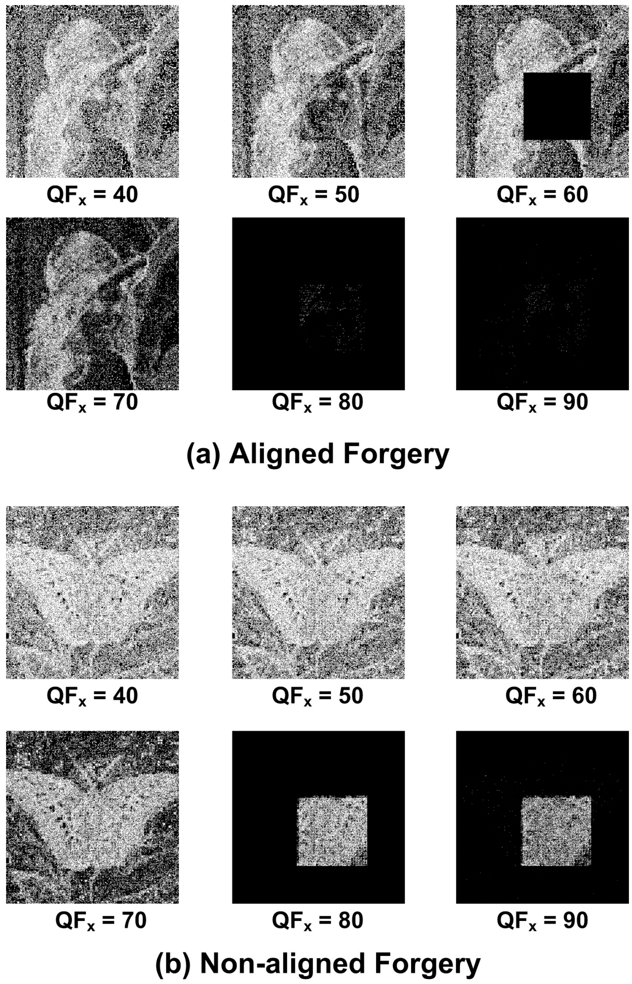


Figure 6.3: S error matrices at different compression ratios $QF_x \in [40, 90]$, shown as grayscale error images. (a) *Lena* in Aligned forgery case. (b) *Butterfly* in Non–aligned forgery case.

(a) and for the *Butterfly* test image in Fig. 6.3 (b) for aligned and non–aligned forms of forgery respectively.

For all our test images, we can distinguish the forged region from the rest of the image, most clearly from the error image at some $QF_x \in$ [40,90]. As evident from Fig. 6.3(a), for the *Lena* image with aligned forgery, the best error image is obtained at $QF_x = 60$ and $QF_x = 80$. Whereas, for the *Butterfly* image with non–aligned forgery, the forged region is best distinguishable from the error image at some $QF_x \in$ [80,90], as evident from Fig. 6.3(b).

Next, we further investigate for localization of the forged region. From the results of forgery detection as shown in Fig. 6.3, the best error matrix that depicts the existence of forgery is obtained at $QF_x = 80$ for aligned forgery and either $QF_x = 80$ (or $QF_x = 90$) for non–aligned forgery. Let us denote the optimal quality factor, that generates the optimal error matrix, as QF_o. From the discussion in Section 4.3, for *Lena* and *Butterfly* test images we observed $QF_o = 80$ to be the optimal quality factor. As discussed in Section 4.4 we

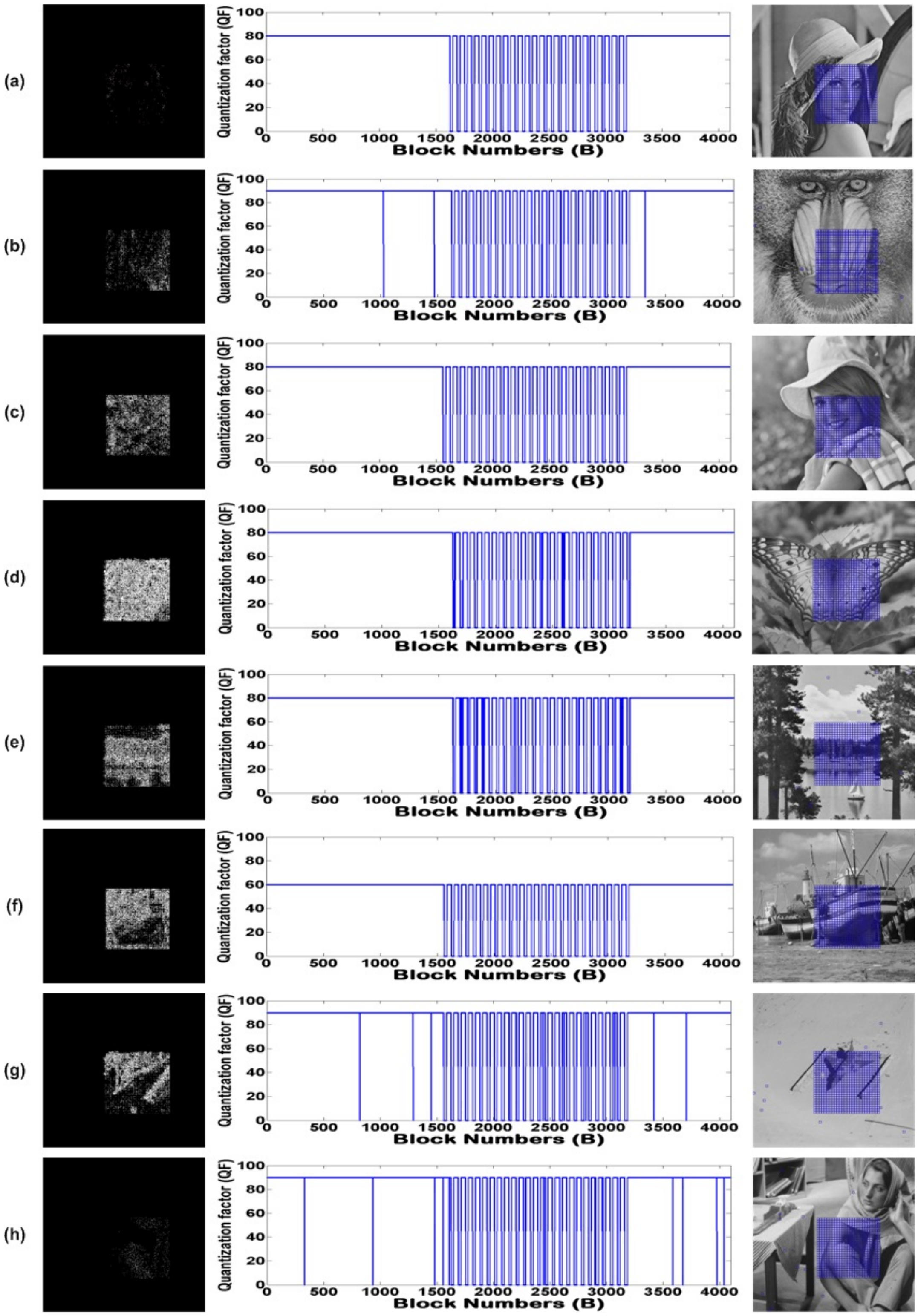


Figure 6.4: Forgery detection and localization results. (Left) Optimal Error Matrices at QF_o. (Center) QF vs. B plots. (Right) Localized forged regions. (a) *Lena* [$QF_o = 80$] (b) *Mandrill* [$QF_o = 90$] (c) *Elaine* [$QF_o = 80$] (d) *Butterfly* [$QF_o = 80$] (e) *Lake* [$QF_o = 80$] (f) *Boat* [$QF_o = 60$] (g) *Jetplane* [$QF_o = 90$] (h) *Barbara* [$QF_o = 90$].

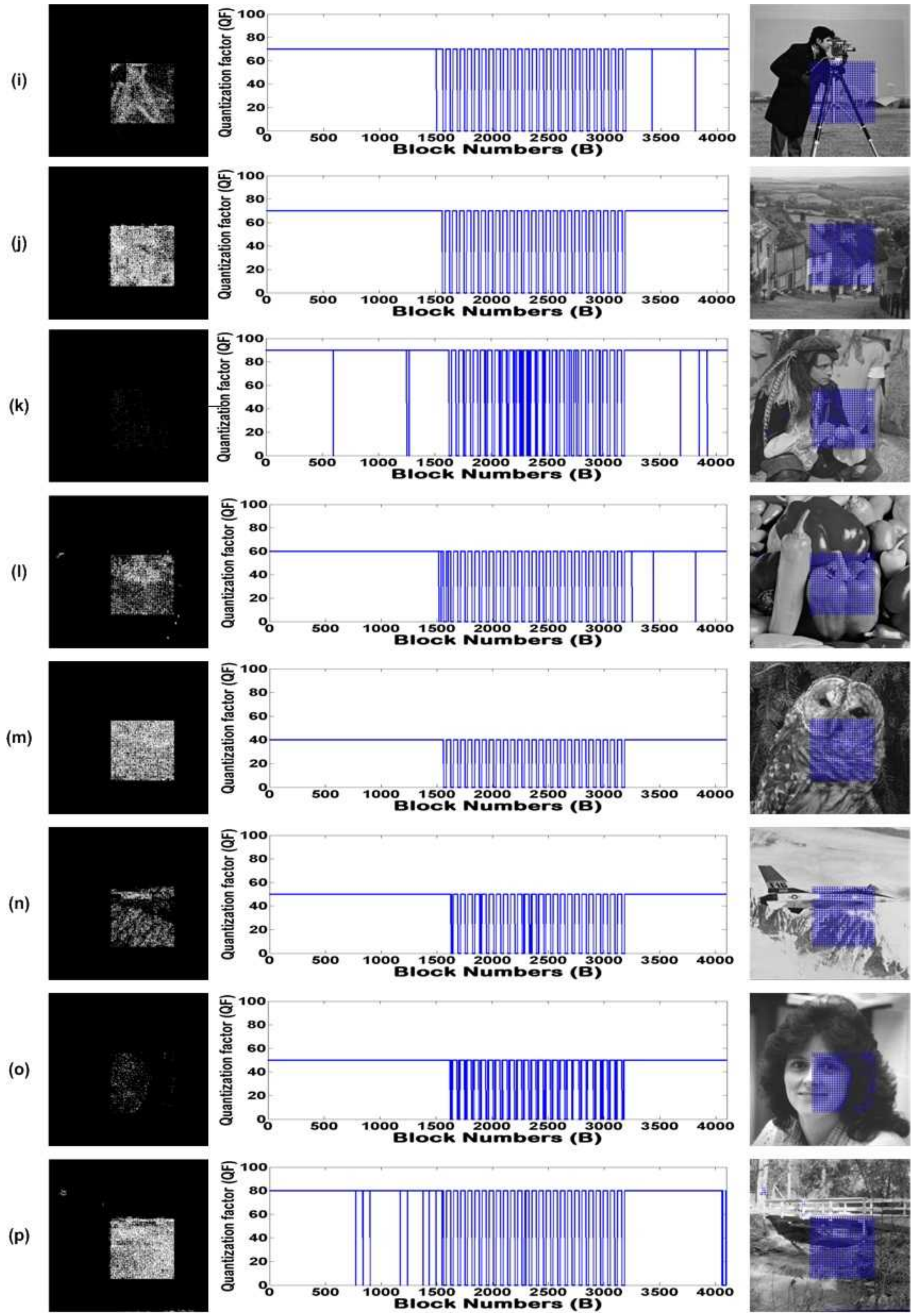


Figure 6.5: Forgery detection and localization results. (Left) Optimal Error Matrices at QF_o. (Center) QF vs. B plots. (Right) Localized forged regions. (i) *Cameraman* $[QF_o = 70]$ (j) *Goldhill* $[QF_o = 70]$ (k) *Pirate* $[QF_o = 90]$ (l) *Peppers* $[QF_o = 60]$ (m) *Owl* $[QF_o = 40]$ (n) *Airplane* $[QF_o = 50]$ (o) *Woman darkhair* $[QF_o = 50]$ (h) *Walkbridge* $[QF_o = 80]$.

utilize the optimal error matrix to localize the forged region.

The optimal error matrix, the QF vs. B plots, and the localization results of the forged test images have been shown in Fig. 6.4. It can be observed that the QF vs. B plot for each test image (for aligned and as well as non–aligned forgery) demonstrates a sudden change that remains persistent over a range of B values, corresponding to the tampered regions of the images. This is in accordance to our discussion in Section 4.4. The pixels locations of the image which are forged, are localized by recording the block indices (B) with the unknown quality factor i.e $QF = 0$.

However certain blocks belonging to the unforged part of the tampered image may be falsely categorized as forged. The QF vs. B plots, in Fig. 6.4 (b), Fig. 6.4 (e), Fig. 6.4 (h), Fig. 6.5 (i), Fig. 6.5 (k), Fig. 6.5 (l) and Fig. 6.5 (p) of the forged test images *Mandrill*, *Lake*, *Barbara*, *Cameraman*, *Pirate*, *Peppers* and *Walkbridge* demonstrate that few blocks belonging to the unforged parts of the images, falsely assumed $QF = 0$. Due to such falsely classified forged blocks, though minimal, we are not always able to achieve 100% detection accuracy. However the proposed detection and localization method achieves an average detection accuracy that is close to 100% and considerably higher when compared with the current state–of–the–art, as we shall see in Section 6.4.

6.2 Detection and Localization of Multiple JPEG Forgeries

In this paper, in addition to a single forgery in an image, we also consider the case where multiple regions of a JPEG image are forged. We consider the general case, where the multiple forgeries involve re-–compressions at varied quality factors. In this experiment, we manually forge multiple regions of our test images. The forgeries induced are of different sizes which are extracted and re-–saved at different quality factors in the range [40,41,...,90]. The forged regions include both aligned and non–aligned types of forgeries.

The proposed detection and localization methods presented in Section 4.2 and Section 4.4 respectively, were applied to the JPEG containing multiple forged regions. The results of this experiment have been presented in Fig. 6.6 for test images (a)–(h) of Fig. 6.1 and in Fig. 6.6 for test images (i)–(p) of Fig. 6.1. The forged regions have been outlined. The optimal error image obtained at $QF_x = QF_o$ depicts the existence of forgeries. QF vs. B plot as well as the localized result of the forged regions has been shown.

6.3 Reconstruction Results of Forged JPEG Images

As discussed in Chapter 5, to reconstruct the tampered test images such that the entire image assumes a uniform compression ratio, we require the knowledge of the ratios at which the regions of the tampered images are compressed.

From the results presented in Section 6.1 for forgery detection and localization, the forged

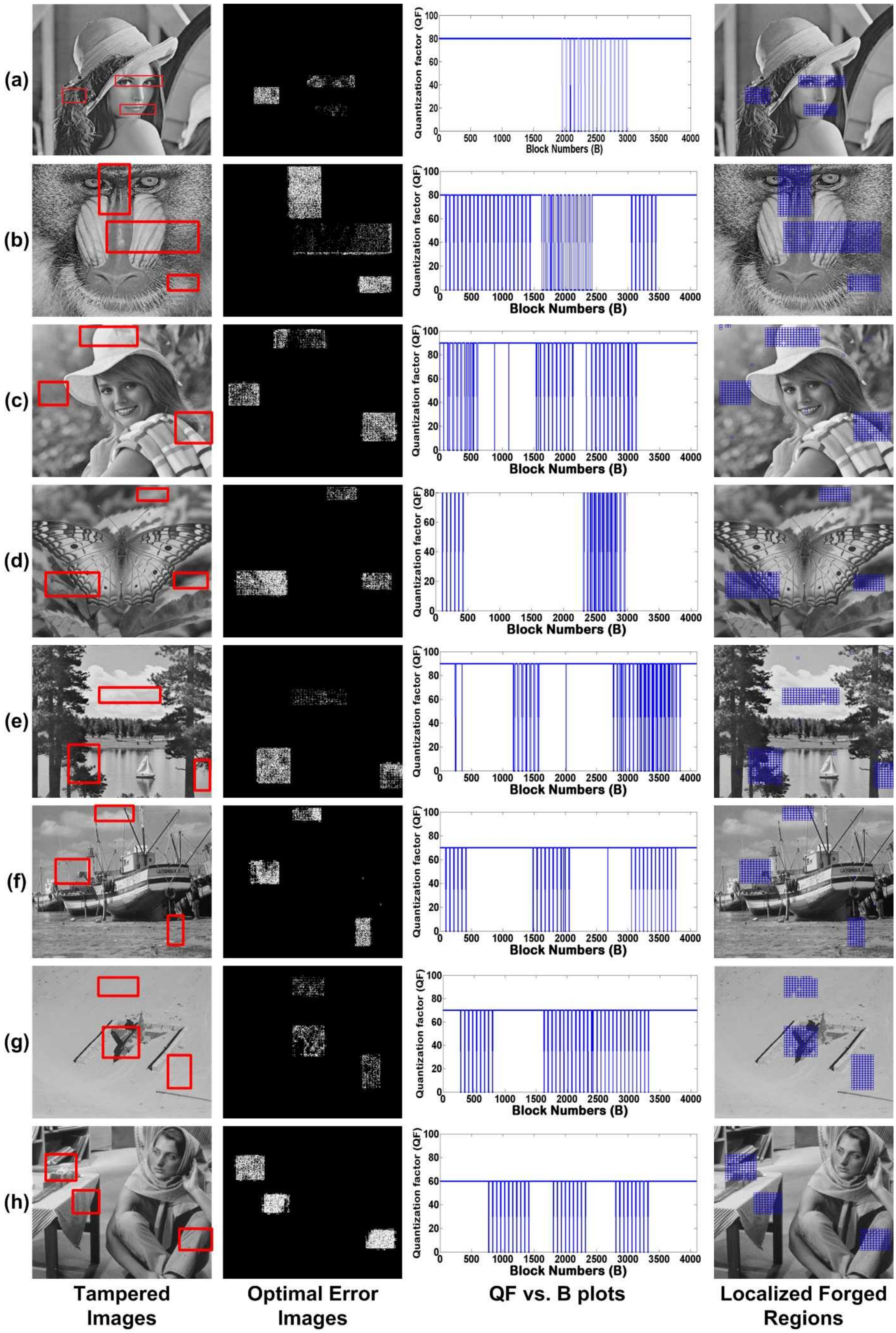


Figure 6.6: Multiple forgeries detection and localization of test images (a)–(h) of Fig. 6.1. From left: The tampered image: (manually) forged regions outlined; Optimal error image depicting the existence of forgery; QF vs. B plot; Localized tampered regions

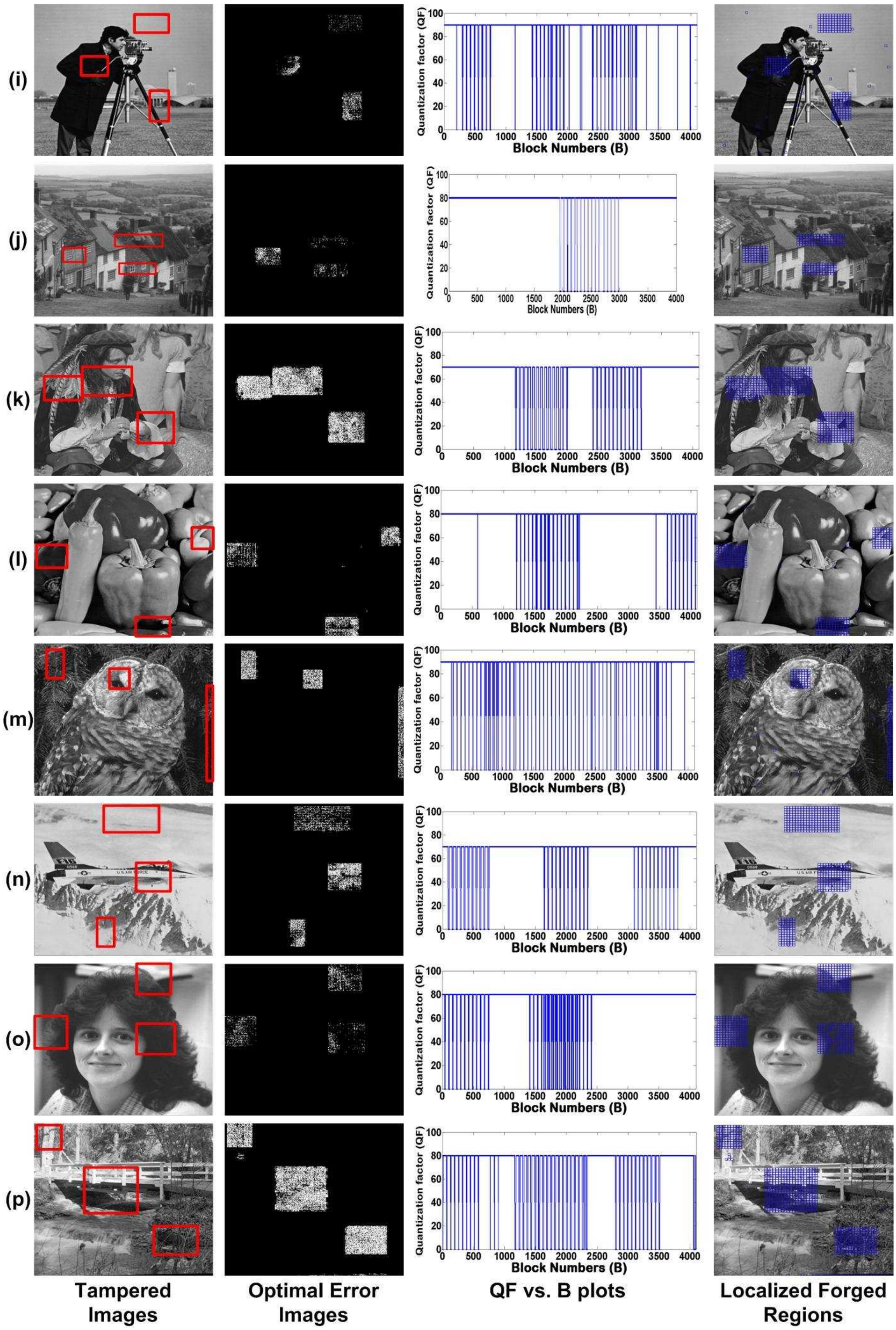


Figure 6.7: Multiple forgeries detection and localization of test images (a)–(h) of Fig. 6.1. From left: The tampered image: (manually) forged regions outlined; Optimal error image depicting the existence of forgery; QF vs. B plot; Localized tampered regions

and unforged regions of a tampered image are successfully identified. Also, the compression ratio at which the unforged region is compressed has been estimated as QF_1, which is nothing but the original test JPEG quality factor. (This is also evident from the QF vs. B plots of Fig. 6.4 and Fig. 6.5.)

On the other hand, to learn the compression ratio of the forged region, the forged region is extracted and re–compressed at different values of quality factor QF_x, ranging from 40 to 90, in steps of 1. The corresponding error images (S matrices) are computed using Eq. 4.1. Next, the consecutive row–-wise horizontal pixel–-pair differences of S are computed and stored into vector D_2 using Eq. 5.1, as discussed in Section 5.1. The D_2 vs. xP plots $\forall\, QF_x \in [40, 90]$ are formed, and out of all those plots, the one obtained with $QF_x = QF_2$ depicts a zero line. Here Px = $[1, 2, \cdots 512 \times 511]$. The D_2 vs. xP plots corresponding to $QF_x = QF_2$ for our test images are shown in second column of Fig. 6.8 for test images (a)–(h) of Fig. 6.1 and Fig. 6.9 for test images (i)–(p) of Fig. 6.1.

The D_2 vs. xP plots of the forged test images are formed by re–compressing them at their original quality factors, i.e., QF_1, and then computing S matrices followed by D_2 vectors, and finally plotting D_2 vs. xP. In the leftmost column of Fig. 6.8 for test images (a)–(h) of Fig. 6.1 and Fig. 6.9 for test images (i)–(p) of Fig. 6.1 for $QF_x = QF_1$ depict the series of plots for the forged test images. The D_2 vs. xP plots demonstrate a sudden change in the D_2 values that remains persistent over a range of pixels corresponding to the forged region.

For reconstruction of the forged images, they have been re–compressed using the technique proposed in Section 5.2 of Chapter 5. For reconstruction, the value of the compression ratio is chosen as that of the forged region, i.e., QF_2. After the proposed reconstruction is carried out, the entire reconstructed image now assumes a uniform compression ratio equal to (QF_1, QF_2) as discussed in Section 5.2. Finally, for verification the D_2 vs. xP plots for the reconstructed images are formed, shown in the rightmost column of Fig. 6.8 for test images (a)–(h) of Fig. 6.1 and Fig. 6.9 for test images (i)–(p) of Fig. 6.1. From those plots it is evident that the reconstructed images assume a uniform compression ratio, (with no sub–part compressed by a compression ratio that differed from rest of the image), since the D_2 vs. xP plots are now zero lines. This is same as the D_2 vs. xP characteristics of the original images.

In addition, to assess the performance of the reconstructed algorithm as well as the visual quality of the optimally reconstructed images, *Structural Similarity Index Measure* (SSIM) and *Peak Signal to Noise Ratio* (PSNR) have been utilized in our work. PSNR is a quality metrix defined as $10 \log_{10}(255^2/MSE)$. The mean squared error (MSE) has been computed between the original image compressed at QF_2, and the optimally reconstructed image. SSIM another a quality metric defined as a measurement of the similarity between two images with a score ranging from 0 to 1 (1 indicates correlation at a maximum and 0 indicates correlation at a minimum between the two corresponding pixels of the original image and the optimally reconstructed image). The PSNR and SSIM values for 16 test images, obtained

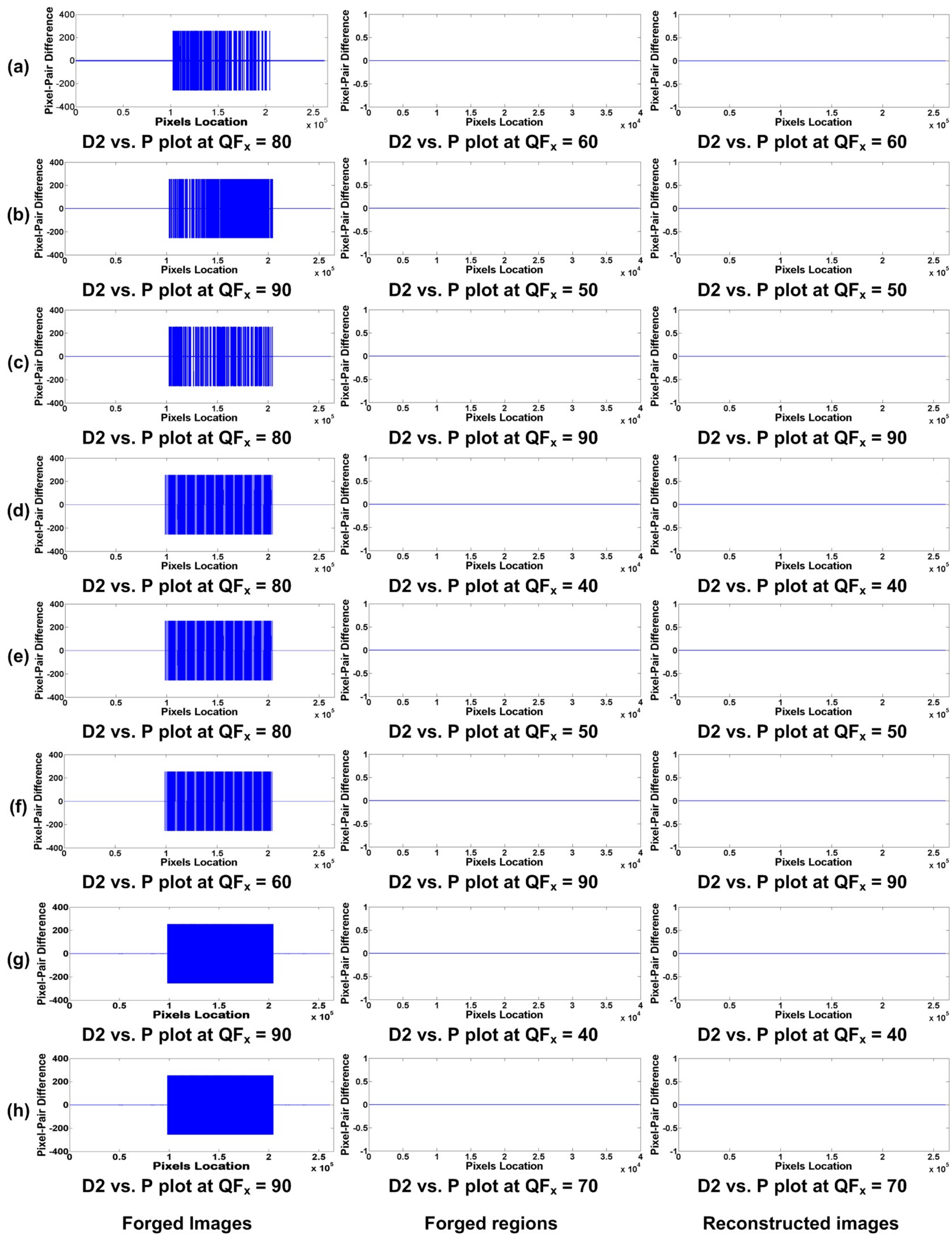


Figure 6.8: D_2 vs. xP plots. (Left) D_2 vs. xP plots for forged images at $QF_x = QF_1$. (Center) D_2 vs. xP plots for forged regions at $QF_x = QF_2$. (Right) D_2 vs. xP plots for reconstructed images at $QF_x = QF_2$. (a) *Lena* $[QF_1 = 80, QF_2 = 60]$ (b) *Mandrill* $[QF_1 = 90, QF_2 = 50]$ (c) *Elaine* $[QF_1 = 80, QF_2 = 90]$ (d)*Butterfly* $[QF_1 = 80, QF_2 = 40]$ (e) *Lake* $[QF_1 = 80, QF_2 = 50]$ (f) *Boat* $[QF_1 = 60, QF_2 = 90]$ (g) *Jetplane* $[QF_1 = 90, QF_2 = 40]$ (h) *Barbara* $[QF_1 = 90, QF_2 = 70]$

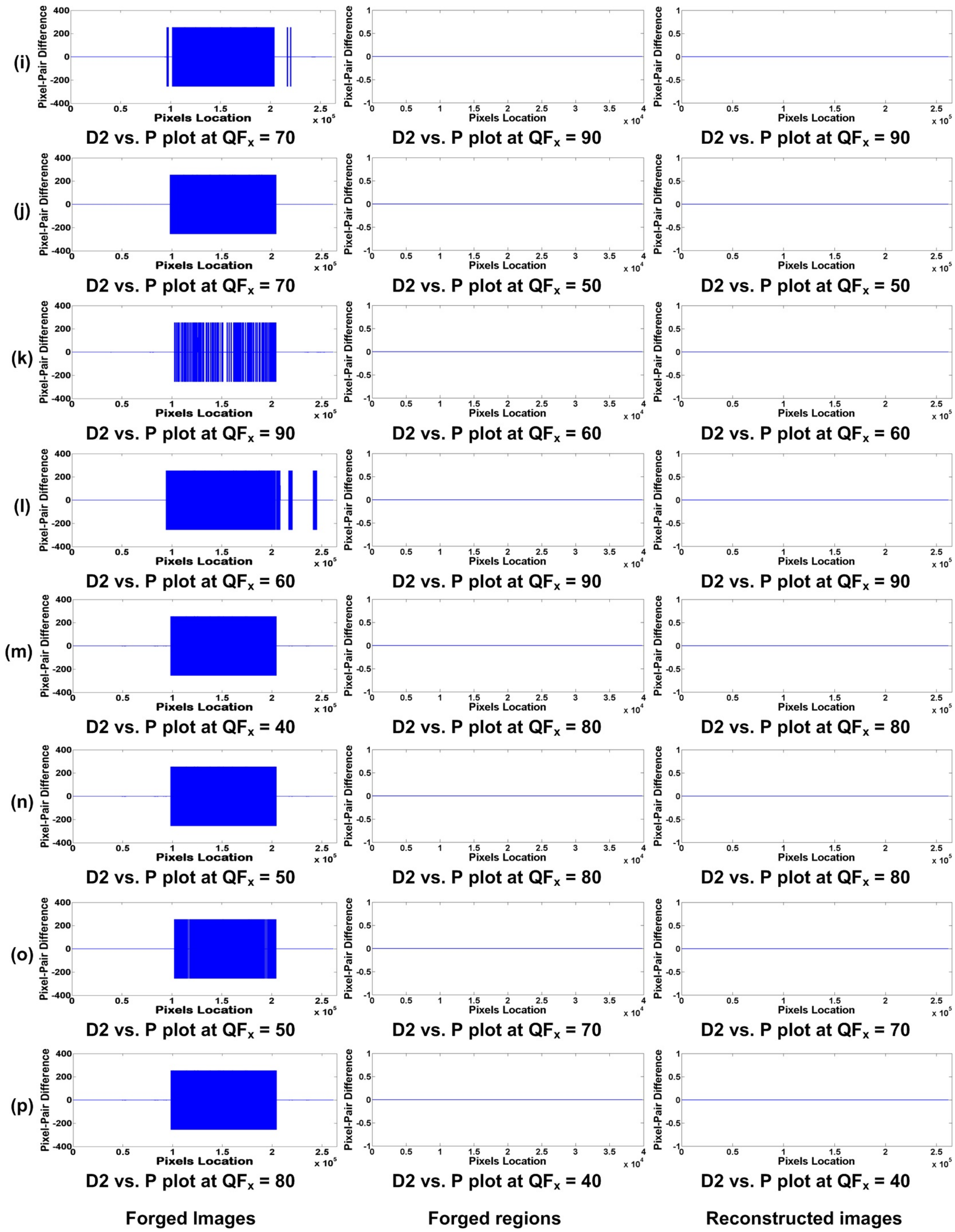


Figure 6.9: D_2 vs. xP plots. (Left) D_2 vs. xP plots for forged images at $QF_x = QF_1$. (Center) D_2 vs. xP plots for forged regions at $QF_x = QF_2$. (Right) D_2 vs. xP plots for reconstructed images at $QF_x = QF_2$. (i) *Cameraman* $[QF_1 = 70, QF_2 = 90]$ (j) *Goldhill* $[QF_1 = 70, QF_2 = 50]$ (k) *Pirate* $[QF_1 = 90, QF_2 = 60]$ (l) *Peppers* $[QF_1 = 60, QF_2 = 90]$ (m) *Owl* $[QF_1 = 40, QF_2 = 80]$ (n) *Airplane* $[QF_1 = 50, QF_2 = 80]$ (o) *Woman darkhair* $[QF_1 = 50, QF_2 = 70]$ (p) *Walkbridge* $[QF_1 = 80, QF_2 = 40]$

Table 6.1: Performance of proposed reconstruction algorithm, averaged over 16 different 512×512 test images, in terms of PSNR and SSIM for Aligned JPEG Compression

QF_1/QF_2		50	60	70	80	90
50	PSNR(dB)	96.89	97.61	91.93	94.39	75.72
	SSIM	1	1	0.99	0.99	0.99
60	PSNR(dB)	90.55	94.69	97.02	88.82	77.97
	SSIM	0.99	0.99	1	0.99	0.99
70	PSNR(dB)	86.66	94.71	96.99	94.46	79.63
	SSIM	0.99	0.99	1	1	0.99
80	PSNR(dB)	95.20	92.90	89.81	96.84	81.36
	SSIM	0.99	0.99	0.99	1	0.99
90	PSNR(dB)	94.57	92.64	94.13	92.84	96.06
	SSIM	0.99	0.99	0.99	0.99	1

by the proposed reconstruction method, are reported in Table. 6.1 for aligned compression forgery and in Table. 6.2 for non–aligned compression forgery . The PSNR and SSIM values are averaged across all the 16 test images that were tampered with different combinations of QF_1 and QF_2 as tabulated in Table. 6.1 and Table. 6.2.

6.4 Comparison with State–of–the–Art

Numerous double compression based JPEG forgery detection methods exist in the current literature, which have been discussed in Chapter 2. Such techniques are specialized to detect re–compression with either aligned or non–aligned block boundaries but not both. The forensic methods presented by Chen and Hsu in [44] and Bianchi et. al in [11] have proposed techniques that can detect both aligned and non–aligned re–compression based forgeries. However the authors in [44] have separately devised two algorithms specialized for these two forms of JPEG forgery. To measure the occurrences of blocking artifacts in non–aligned forgery as well as the DCT coefficients in aligned forgery, a set of features have been defined. Similarly, in [11], the authors have proposed statistical models to descrimintae

Table 6.2: Performance of proposed reconstruction algorithm, averaged over 16 different 512×512 test images, in terms of PSNR and SSIM for Non–aligned JPEG Compression

QF_1/QF_2		50	60	70	80	90
50	PSNR(dB)	43.05	43.69	44.05	46.23	49.91
	SSIM	1	0.99	0.99	0.99	0.99
60	PSNR(dB)	41.37	43.75	44.66	46.52	49.78
	SSIM	0.98	0.99	0.99	0.99	0.99
70	PSNR(dB)	39.29	41.57	44.63	45.26	49.54
	SSIM	0.98	0.98	0.99	0.99	0.99
80	PSNR(dB)	41.09	39.22	41.59	45.83	49.24
	SSIM	0.98	0.97	0.98	0.99	0.99
90	PSNR(dB)	40.94	41.11	42.36	41.08	48.32
	SSIM	0.98	0.98	0.98	0.98	0.99

forgery based on quantized DCT coefficients for aligned compression and dequantized DCT coefficients for non–aligned compression are used to discriminate aligned and non–aligned JPEG forgeries. have been used as features to discriminate forgeries. Also, most methods such as [Luo et al. 2007; Bianchi and Piva 2011; 2012a; 2012b], require suspecting and cropping a region to check for existence of forgery.

Our contribution in this paper, is a generalized technique that can detect the existence of both forms of forgeries: aligned and non–aligned and does not require suspecting and cropping a region to detect the forgery. Importantly, when an image has been tampered with both forms of forgeries at multiple regions, our method is efficient enough to detect all. Majority of the existing algorithms analyze the whole image to detect the presence of forgery, without localizing the actual tampered region. However, to the best of our knowledge the forensic algorithms in [Bianchi and Piva 2012b; Bianchi et al. 2011; He et al. 2006; Wang et al. 2011] automatically detect and localize forged regions. In the paper, we propose a forensic JPEG forgery localization algorithm where we require no a–priori information related to the image area that underwent tampering, and operates efficiently for single as well as multiple JPEG compression of degree two based forgeries, adhering to both aligned or non–aligned or both.

Table 6.3: Comparision results of the proposed forgery detection and localization algorithm with state-of–the–art in terms of Detection Accuracy (DA) for Aligned JPEG Forgery.

QF_1/ QF_2		50	60	70	80	90
50	Proposed	28.25	**99.47**	**99.21**	**99.11**	98.77
	[44]	64	91	97	99	**100**
	[24]	59	69	97	98	99
	[20]	0.84	59.3	84.0	94.0	96.8
60	Proposed	**99.56**	32.60	**99.61**	**99.32**	**99.02**
	[44]	86	**68**	96	**99**	**100**
	[24]	83	56	90	**100**	**99**
	[20]	45.8	1.12	72.7	96.6	97.0
70	Proposed	**99.60**	**99.66**	32.57	**99.61**	**99.48**
	[44]	75	87	71	**99**	**100**
	[24]	70	60	66	96	**100**
	[20]	37.8	41.3	1.92	74.3	95.1
80	Proposed	**98.78**	**99.60**	**99.78**	32.57	**99.40**
	[44]	84	84	79	66	**100**
	[24]	67	59	61	62	**100**
	[20]	47.6	39.5	32.8	4.03	94.2
90	Proposed	**98.47**	**98.75**	**99.19**	**99.22**	**84.23**
	[44]	71	75	67	88	77
	[24]	64	59	63	50	68
	[20]	40.5	40.5	44.2	40.5	12.8

To prove the efficiency of the proposed work we evaluated the performance of the proposed forgery detection and localization techniques, and compared it with six other JPEG forensic techniques. The performance has been measured in term of detection accuracy, separately for aligned and non–aligned forgery cases.

For aligned forgery detection, we have compared our Detection Accuracy (DA) results with those of [20, 24, 44]. The DA results achieved for different combinations of (QF_1,QF_2) are tabulated in Table 6.4. In case of non–aligned forgery we have compared our proposed technique with [22, 43, 44]. The DA results for different combination of (QF_1,QF_2) are tabulated in Table 6.4. The performance results presented in Table 6.4, represents the performance averaged over our entire test set. In Table 6.4, for each combination of

Table 6.4: Comparision results of the proposed forgery detection and localization algorithm with state-of–the–art in terms of Detection Accuracy (DA) for Non-Aligned JPEG Forgery.

QF_1/ QF_2		50	60	70	80	90
50	Proposed	**98.59**	**98.62**	**98.62**	**98.64**	**98.67**
	[43]	88.5	92.6	93.7	94.7	95.7
	[44]	56.3	62.4	73.7	82.4	91.5
	[22]	73.6	82.6	89.5	95.9	97.1
60	Proposed	**98.60**	**98.63**	**98.68**	**98.67**	**98.68**
	[43]	80.7	90.7	94.4	96.3	97.2
	[44]	55.1	60.0	67.6	79.3	90.6
	[22]	67.2	77.3	85.4	94.8	97.2
70	Proposed	**98.59**	**98.63**	**98.65**	**98.66**	**98.68**
	[43]	60.8	77.7	92.5	96.5	98.0
	[44]	53.2	56.7	61.9	72.7	88.6
	[22]	61.0	67.8	76.8	89.9	97.3
80	Proposed	**98.56**	**98.64**	**98.67**	**98.68**	**98.68**
	[43]	50.2	53.6	67.6	91.0	98.6
	[44]	51.4	753.5	57.1	63.1	80.7
	[22]	57.4	60.0	63.9	75.3	94.8
90	Proposed	**98.25**	**98.29**	**98.34**	**98.35**	**98.36**
	[43]	50.2	50.1	49.8	54.8	85.4
	[44]	49.5	49.8	50.8	53.3	63.5
	[22]	55.4	52.8	53.4	56.4	76.5

(QF_1,QF_2), the highest DA achieved among the four techniques has been highlighted in bold.

As evident from Table. 6.4, in case of aligned forgery, our proposed scheme outperforms [20, 24, 44] when $QF_1 \neq QF_2$, with DA values close to 100%. Moreover, in [20], the method is effective only in those tampered images where the region has been tampered with a quality factor comparatively lower than the rest of the image, which is not any limitation in the proposed method as evident from Table. 6.4. However, for $QF_1 = QF_2$, since the DCT coefficients do not get modified after re–compression, the proposed method does not always achieve equally high detection accuracy for this form of re–compression. For non–aligned forgery detection, the proposed scheme outperforms [22, 43, 44] for all cases $QF_1 < QF_2$, $QF_1 = QF_2$ and $QF_1 > QF_2$, with DA close to 100%, as evident from Table. 6.4.

6.5 Summary

Our experimental results for the proposed forgery and localization techniques as well as for the reconstruction technique have been assessed in this chapter. Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) have been utilized as quality metric measurement for our reconstructed images. Also comparison with the state–of–the–art JPEG forensic techniques [1]–[5] to prove the efficiency of our method have been evaluated in terms of average detection accuracy. Our experimental results achievied detection accuracy close to 100%.

Chapter 7

Conclusion and Future Work

In this thesis, we propose a blind JPEG forgery detection and localization technique, which attains three–way goal. First, it enables the forgery detection and localization processes to be completely automated without the need for human intervention. Second, single as well as multiple forged regions are detectable with our detection and localization approaches. Finally we propose an optimal reconstruction technique for forged JPEG images.

We have dealt with two classes of JPEG image forgery, viz., aligned and non–aligned double JPEG compressions. The inherent characteristics of JPEG compression and the effects of re–-compression have been exploited in forms of S error images, QF vs. B plots and D2 vs. Px plots of JPEG tampered images, in order detect and localize forgery as well as to reconstruct forged JPEG images.

For our forgery detection approach we investigate the S error images. We find the optimal error–matrix for which most of its entries $S(i, j) = 0$. The optimal error–matrix clearly depicts the existence of forgery in a tampered image.

In order to localize the forgery we utilize the optimal error matrix where we divide the tampered image into blocks of $8 \times 8 pixels$ and quality factor (QF) of the each tampered image block are estimated. The QF vs. B plot is used to localize the forgeries by locating those blocks with unknown quality factor.

To reconstruct the forged image we utilize the characteristics of the pixel–differences D_2 computed from the S error matrix. The $D2$ vs. Px plot of a reconstructed JPEG image demonstrates a zero line consistent to that of an original image thereby indicating that our proosed reconstruction method achieves the aim of optimally reconstructing the tampered image with its entire region subsequently compressed uniformly with the same quality factor.

Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) have been used as performance metric as well as quality metric to efficiency of the proposed reconstruction method as well as the visual quality of the optimally reconstructed image. To prove the efficiency of the proposed forgery and detection techniques evaluated its performance and compared it with the state–of–the–art JPEG forensic techniques [1]–[5]. Our experimental results prove the efficiency of our proposed techniques with detection accuracy close to 100%.

Future Work

This thesis solely deals with double compression based JPEG forgery detection. However JPEG forged image can also involve re–compression of higher degrees. For example a triple JPEG compressed image where an image has undergone three times compression. The future direction of this research includes investigation of JPEG forgeries involving triple or higher degrees of compression.

Also in reality, multiple manipulating operations are used to create a forgery. Most of the existing digital forensic techniques are devised to detect specific type of manipulating. In future a further study on the different types of image manipulating operations will be done so as to identify the fingerprints or evidences that is left behind in a tampered image. Based on the findings a robust forensics techniques can be devised in the future.

References

[1] A. Images. (2014) Is obama 'listening' to india's modi? [Online]. Available: http://www.bbc.com/news/blogs-news-from-elsewhere-26087143

[2] H. T. Sencar and N. Memon, *Digital image forensics: There is more to a picture than meets the eye*. Springer Science & Business Media, 2012.

[3] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: a booklet for beginners," *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133–162, 2011.

[4] H. Farid, "Image forgery detection," *Signal Processing Magazine, IEEE*, vol. 26, no. 2, pp. 16–25, 2009.

[5] H. T. Sencar and N. Memon, "Overview of state-of-the-art in digital image forensics," *Algorithms, Architectures and Information Systems Security*, vol. 3, pp. 325–348, 2008.

[6] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389–399, 2010.

[7] X. Pan and S. Lyu, "Detecting image region duplication using sift features," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1706–1709.

[8] W. Zhang, X. Cao, J. Zhang, J. Zhu, and P. Wang, "Detecting photographic composites using shadows," in *Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on*. IEEE, 2009, pp. 1042–1045.

[9] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind source camera identification," in *Image Processing, 2004. ICIP'04. 2004 International Conference on*, vol. 1. IEEE, 2004, pp. 709–712.

[10] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in *Electronic Imaging 2006*. International Society for Optics and Photonics, 2006, pp. 60 720Y–60 720Y.

[11] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of jpeg artifacts," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 3, pp. 1003–1017, 2012.

[12] C. Podilchuk, E. J. Delp *et al.*, "Digital watermarking: algorithms and applications," *Signal Processing Magazine, IEEE*, vol. 18, no. 4, pp. 33–46, 2001.

[13] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*. Morgan Kaufmann, 2007.

[14] F. Y. Shih, *Digital watermarking and steganography: fundamentals and techniques*. CRC Press, 2007.

[15] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press, 2009.

[16] T. Pevnỳ and J. Fridrich, "Detection of double-compression in jpeg images for applications in steganography," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 2, pp. 247–258, 2008.

[17] T.-T. Ng, S.-F. Chang, C.-Y. Lin, and Q. Sun, "Passive-blind image forensics," *Multimedia Security Technologies for Digital Rights*, vol. 15, pp. 383–412, 2006.

[18] G. K. Wallace, "The jpeg still picture compression standard," *Consumer Electronics, IEEE Transactions on*, vol. 38, no. 1, pp. xviii–xxxiv, 1992.

[19] A. B. Watson, *Digital images and human vision*. MIT press, 1993.

[20] H. Farid, "Exposing digital forgeries from jpeg ghosts," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 1, pp. 154–160, 2009.

[21] P. Malviya and R. Naskar, "Digital forensic technique for double compression based jpeg image forgery detection," in *Information Systems Security*. Springer, 2014, pp. 437–447.

[22] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*, vol. 2. IEEE, 2007, pp. II–217.

[23] D. Fu, Y. Q. Shi, and W. Su, "A generalized benford's law for jpeg coefficients and its applications in image forensics," in *Electronic Imaging 2007*. International Society for Optics and Photonics, 2007, pp. 65 051L–65 051L.

[24] B. Li, Y. Q. Shi, and J. Huang, "Detecting doubly compressed jpeg images by using mode based first digit features," in *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*. IEEE, 2008, pp. 730–735.

[25] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Information Hiding*. Springer, 2005, pp. 128–147.

[26] J. Lukáš and J. Fridrich, "Estimation of primary quantization matrix in double compressed jpeg images," in *Proc. Digital Forensic Research Workshop*, 2003, pp. 5–8.

[27] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered jpeg image detection via dct coefficient analysis," *Pattern Recognition*, vol. 42, no. 11, pp. 2492–2501, 2009.

[28] T. Bianchi, A. De Rosa, and A. Piva, "Improved dct coefficient analysis for forgery localization in jpeg images," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011, pp. 2444–2447.

[29] A. T. Ho and S. Li, *Handbook of Digital Forensics of Multimedia Data and Devices*. John Wiley & Sons, 2015.

[30] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, *Digital watermarking*. Springer, 2002, vol. 53.

[31] C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on Applied Signal Processing*, vol. 6, pp. 613–621, 2002.

[32] J. Fridrich, "Methods for tamper detection in digital images," in *Multimedia and Security, Workshop at ACM Multimedia*, vol. 99, 1999, pp. 29–34.

[33] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing jpeg compression from malicious manipulation," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 11, no. 2, pp. 153–168, 2001.

[34] M. Schneider and S.-F. Chang, "A robust content based digital signature for image authentication," in *Image Processing, 1996. Proceedings., International Conference on*, vol. 3. IEEE, 1996, pp. 227–230.

[35] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on dct and svd," *Forensic science international*, vol. 233, no. 1, pp. 158–166, 2013.

[36] Z. Qu, G. Qiu, and J. Huang, "Detect digital image splicing with visual cues," in *Information Hiding*. Springer, 2009, pp. 247–261.

[37] B. Mahdian and S. Saic, "Detecting double compressed jpeg images," in *Crime Detection and Prevention (ICDP 2009), 3rd International Conference on*. IET, 2009, pp. 1–6.

[38] Y.-L. Chen and C.-T. Hsu, "Image tampering detection by blocking periodicity analysis in jpeg compressed images," in *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*. IEEE, 2008, pp. 803–808.

[39] S. Ye, Q. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Multimedia and Expo, 2007 IEEE International Conference on*. IEEE, 2007, pp. 12–15.

[40] W. Junwen, L. Guangjie, D. Yuewe, and W. Zhiquan, "Detecting jpeg image forgery based on double compression," *Systems Engineering and Electronics, Journal of*, vol. 20, no. 5, pp. 1096–1103, 2009.

[41] Y.-L. Chen and C.-T. Hsu, "Detecting doubly compressed images based on quantization noise model and image restoration," in *Multimedia Signal Processing, 2009. MMSP'09. IEEE International Workshop on*. IEEE, 2009, pp. 1–6.

[42] T. Bianchi and A. Piva, "Detection of non-aligned double jpeg compression with estimation of primary compression parameters," in *Image Processing (ICIP), 2011 18th IEEE International Conference on*. IEEE, 2011, pp. 1929–1932.

[43] ——, "Detection of nonaligned double jpeg compression based on integer periodicity maps," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 842–848, 2012.

[44] Y.-L. Chen and C.-T. Hsu, "Detecting recompression of jpeg images via periodicity analysis of compression artifacts for tampering detection," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 2, pp. 396–406, 2011.

[45] V. L. Thing, Y. Chen, and C. Cheh, "An improved double compression detection method for jpeg image forensics," in *Multimedia (ISM), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 290–297.

[46] L. Wu, X. Kong, B. Wang, and S. Shang, "Image tampering localization via estimating the non-aligned double jpeg compression," *Proceedings of IS&T/SPIE Electronic Imaging, pp. 86650R1–86650R7*, 2013.

[47] J. He, Z. Lin, L. Wang, and X. Tang, "Detecting doctored jpeg images via dct coefficient analysis," in *Computer Vision–ECCV 2006*. Springer, 2006, pp. 423–435.

[48] W. Wang, J. Dong, and T. Tan, "Tampered region localization of digital color images based on jpeg compression noise," in *Digital Watermarking*. Springer, 2011, pp. 120–133.

[49] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y.-Q. Shi, "An effective method for detecting double jpeg compression with the same quantization matrix," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 11, pp. 1933–1942, 2014.

[50] R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics," in *Digital Image Forensics*. Springer, 2013, pp. 327–366.

[51] F. Chunhui, Z. Xinghui *et al.*, "An anti-forensic algorithm of jpeg double compression based forgery detection," in *Information Science and Engineering (ISISE), 2012 International Symposium on*. IEEE, 2012, pp. 159–164.

[52] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. R. Liu, "Anti-forensics of jpeg compression," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1694–1697.

[53] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. Liu, "Undetectable image tampering through jpeg compression anti-forensics," in *Image Processing (ICIP), 2010 17th IEEE International Conference on*. IEEE, 2010, pp. 2109–2112.

[54] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "A variational approach to jpeg anti-forensics," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*. IEEE, 2013, pp. 3058–3062.

[55] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, “Countering jpeg anti-forensics,” in *Image Processing (ICIP), 2011 18th IEEE International Conference on*. IEEE, 2011, pp. 1949–1952.

[56] S. Lai and R. Böhme, “Countering counter-forensics: the case of jpeg compression,” in *Information hiding*. Springer, 2011, pp. 285–298.

[57] D. A. Huffman *et al.*, “A method for the construction of minimum redundancy codes,” *Proceedings of the IRE*, vol. 40, no. 9, pp. 1098–1101, 1952.

[58] S. Manimurugan and B. Jose, “A novel method for detecting triple jpeg compression with the same quantization matrix,” *International Journal of Engineering Trends and Technology*, vol. 3, no. 2, pp. 94–97, 2012.

[59] CVG-UGR. (2007) The cvg-ugr image database. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/g512.php

[60] A. G. Weber. (1997) The usc-sipi image database. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc

Dissemination

Journal Publication

1. D. B. Tariang and R. Naskar, ”Multiple–compression based JPEG Forgery Detection and Optimal Reconstruction” under Major Revision in ACM Transactions on Multimedia Computing, Communications, and Applications.

Conference Publication

1. D. B. Tariang and R. Naskar, ”Re–Compressed based JPEG Forgery Detection and Localization through Automated Quality Factor Investigation”, *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 23–25 March 2016.*
   `The paper has been recommended for consideration and possible publication in the WiSPNET Special Issue journal (AEÜ - International Journal of Electronics and Communications).`